TERANAS INSTANT STORAGE

User Guide

SnaZio*

TERA NAS HD PRO

Copyright © 2005, **V One Multimedia**. All rights reserved.

http://www.Snazio.com

Contents

About This Guide ---------- 7

1. FrontView Advanced Control ---------- 8

Clock ---------- 11

System Time ---------- 11

NTP Option ---------- 12

Network ---------- 13

Ethernet ---------- 13

Wireless ---------- 14

DNS ---------- 16

WINS ---------- 16

DHCP ---------- 18

Route ---------- 20

Security ---------- 21

Share Mode ---------- 23

Specify a Workgroup ---------- 23

User Mode ---------- 24

Specify a Workgroup ---------- 25

Setting up Accounts ---------- 25

Managing Groups ---------- 26

Managing Users ---------- 27

Settings Accounts Defaults ---------- 30

Domain Mode ---------- 31

Domain/ ADS Authentication ---------- 31

Shares ---------- 32

Services ---------- 32

Adding Shares ---------- 33
Managing Shares ---------- 35
Setting Share Access in Share Mode ---------- 37
Setting Share Access in User and Domain Modes ---------- 38
Taking and Scheduling Snapshot ---------- 40
Volume Management ---------- 44
Deleting a Volume ---------- 44
Adding a Volume ---------- 45
RAID Settings ---------- 48
Printers ---------- 49
Systems ---------- 51
Alerts ---------- 51
Alerts Contacts ---------- 51
Alerts Settings ---------- 52
SNMP ---------- 52
SMTP ---------- 54
Admin Password ---------- 55
Performance ---------- 57
Adding a UPS for performance ---------- 58
Language ---------- 59
Updating TeraNAS ---------- 61
Remote Update ---------- 61
Local Update ---------- 63
Factory Default ---------- 63
Shutdown ---------- 64
Status ---------- 66
Logs ---------- 66

Health ---------- 66

2. Accessing Shares ---------- 68

Windows ---------- 69

MAC OS X ---------- 71

MAC OS 9 ---------- 75

Linux/ UNIX ---------- 77

Web Browser ---------- 78

FTP 81

3. Replacing a Failed Disk ---------- 82

Locate the Failed Disk ---------- 82

Order Replacement Disk ---------- 83

Replace the Failed Disk ---------- 83

Resynchronize the Volume ---------- 84

4. System Reset Switch ---------- 85

A. Streaming Videos Using SnaZio* Tera Nas HD Pro ---------- 87

Introductions ---------- 87

Network Connections ---------- 87

Managing Media Contents ---------- 89

Managing Media Files ---------- 91

B. Changing User Password ---------- 93

C. RAID Levels Simplified ---------- 94

RAID Level 0 ---------- 95

RAID Level 1 ---------- 95

RAID Level 5 ---------- 96

D. Input Field Format ---------- 96

Domain/ Workgroup Names ---------- 96

Host ---------- 97

Host Name ---------- 97

TeraNAS Host Name ---------- 97

Host Expression ---------- 97

Share Name ---------- 98

Share Password ---------- 98

SNMP Community ---------- 98

User/Group Name ---------- 99

User Password ---------- 99

E. Glossary ---------- 100

F. If You Need Help ---------- 101

About This Guide

Congratulations and thank you for purchasing a TeraNAS Instant Storage system from V One Multimedia. If you haven't already done so, please read the *Getting Started* guide provided in the shipping box and the *Quick Installation Guide* on the CD-ROM.

Where the *Quick Installation Guide* takes you through step-by-step through the FrontView Setup Wizard and quickly prepares the TeraNAS for your network, the *User Guide* explains each of the available option in detail, including a lot of advanced options not available during the Setup Wizard process.

Chapter 1, "FrontView Advanced Control", describes all the menus and tabs available in the Advanced Control mode.

If you have configured the TeraNAS and you need help in accessing the shares on the TeraNAS, skipt to Chapter 2, "Accessing Shares".

If you have encountered a disk failure, you need to know the proper procedure for replacing the failed disk. Chapter 3, "Replacing a Failed Disk", covers this.

If you have problems that you or the technical support team is not able to resolve, perhaps re-installing the firmware or resetting the system back to factory default might help. Chapter 4, "System Reset Switch", explains the process of doing both.

Most people are unaware of the benefits or the differences between the RAID levels that the TeraNAS supports. Appendix A, "RAID Levels Simplified", explains the levels without going too deep in detail.

If you have questions on what constitutes a valid input for host name, workgroup, or password, Appendix B, "Input Field Format", describes these and more.

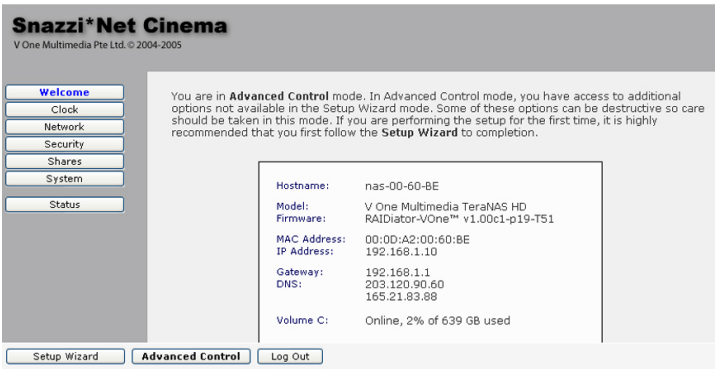
Appendix C, "Glossary", provides the definition for some of the technical terminologies used in this document.

If you need help during setup, refer to Appendix D, "If You Need Help…".

Chapter 1 FrontView Advanced Control

The Advanced Control mode offers the options available in the Setup Wizard plus more.

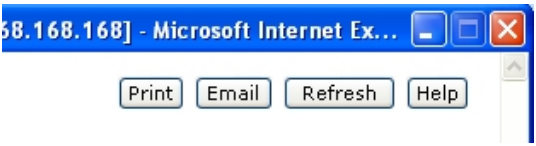
Welcome


Snazzi*Net Cinema
V One Multimedia Pte Ltd. © 2004-2005
Welcome
Clock
Network
Security
Shares
System
Status
You are in Advanced Control mode. In Advanced Control mode, you have access to additional options not available in the Setup Wizard mode. Some of these options can be destructive so care should be taken in this mode. If you are performing the setup for the first time, it is highly recommended that you first follow the Setup Wizard to completion.
Hostname: nas-00-60-BE
Model: V One Multimedia TeraNAS HD
Firmware: RAIDiator-VOne™ v1.00c1-p19-T51
MAC Address: 00:0D:A2:00:60:BE
IP Address: 192.168.1.10
Gateway: 192.168.1.1
DNS: 203.120.90.60
165.21.83.88
Volume C: Online, 2% of 639 GB used
Setup Wizard
Advanced Control
Log Out

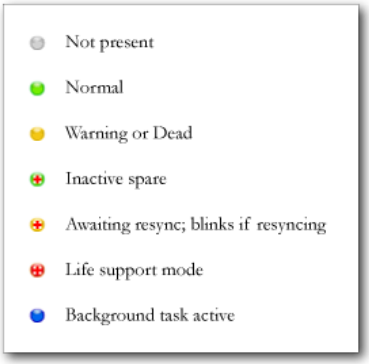
When you first switch to this mode, you'll notice the menus on the left that allow you to quickly jump to the desired menu page. Towards the

bottom left, you'll notice buttons that allow you to switch back and forth between Setup Wizard mode and Advanced Control mode.

As you click on the menu buttons, you'll notice a similar theme across all menu pages. At the top right corner is the command bar which typically provides options to print or email the page, refresh the browser window, and display help where available.



At the furthest bottom is the **status bar** with the date button which doubles its duty as a clock and a link to the **Clock** page. The status LEDs to the right gives a quick glimpse of the enclosure device status.



The status represent:

- **Not present** – No disk or device attached.

- **Normal** – Device in normal operating mode.
- **Warning or Dead** – The device has failed or is in a state where it needs attention.
- **Inactive spare** – This disk is a spare disk on standby. If a disk fails, this disk will take over automatically.
- **Awaiting resync; blinks if resyncing** – This disk is waiting to resync to the RAID volume. If the LED is blinking, this disk is currently resyncing. During resync process, volume is in degraded mode – performance is effected by the resync process and another disk failure in the volume will render it dead.
- **Life support mode** – The volume has encountered multiple disk failures and is in the state of being marked dead. However, the TeraNAS has blocked it from being marked dead in the event that someone may have accidentally pulled out the wrong disk during runtime. If the wrong disk was pulled out, shutdown the TeraNAS immediately, reconnect the disk, and power-on the TeraNAS. If you reconnect the disk during runtime, the TeraNAS will mark it as a newly added disk and you will no longer be able to access the data on it.
- **Background task active** – A lengthy background task such as a system update is in progress.

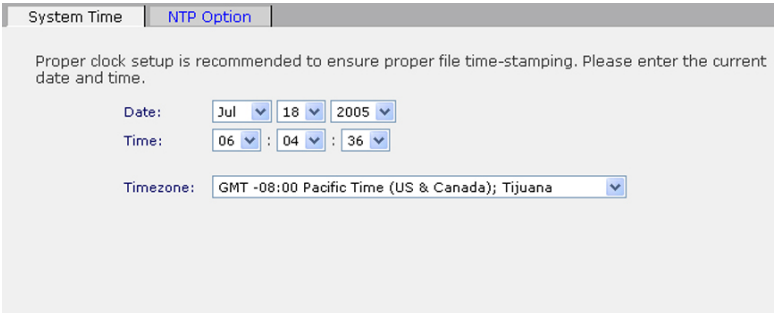
Hover the mouse cursor over the LED to display more information on the device, or click on it to display the status in more detail.

Right above the status bar is the **action bar**. To the left is the Logout button. Due to security reasons, the **Logout** button only acts as a reminder to close the current browser session which is necessary to securely log out. To the right is the **Apply** button. Use this to save any changes in the current menu page.

Clock

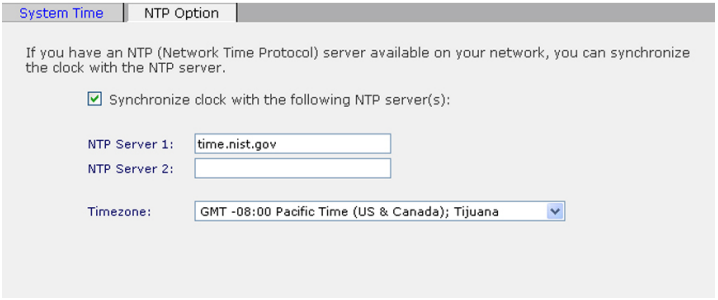
System Time

The System Time tab in the Clock page allows you to set the date, time, and time zone. Set appropriately to ensure files maintain proper timestamp.



NTP Option

You can elect to synchronize the system time on the device with a remote NTP (Network Time Protocol) server. Click on the **NTP Options** tab to designate the host name or IP address of the NTP server. You can elect to keep the default server or enter a NTP server closer to your locale. Available public NTP servers can be found by searching the web.

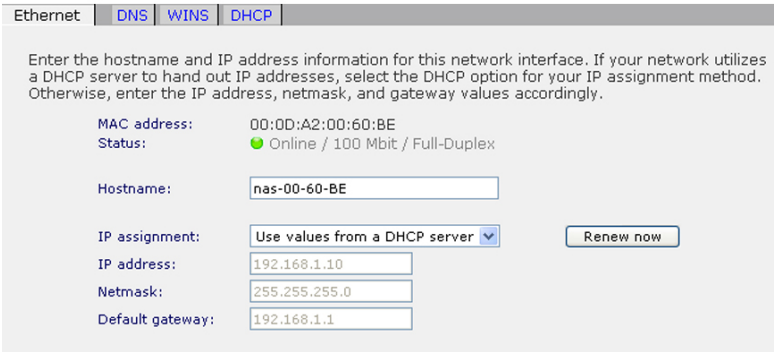

System Time
NTP Option
If you have an NTP (Network Time Protocol) server available on your network, you can synchronize the clock with the NTP server.
Synchronize clock with the following NTP server(s):
NTP Server 1:
time.nist.gov
NTP Server 2:
Timezone:
GMT -08:00 Pacific Time (US & Canada); Tijuana

Network

Ethernet

The Ethernet tab allows you to set the hostname, IP address, network mask, and default gateway for your TeraNAS device. In most networks where a DHCP service is offered, you can simply specify the "Use values from a DHCP server" option to automatically set the latter three options.

Network



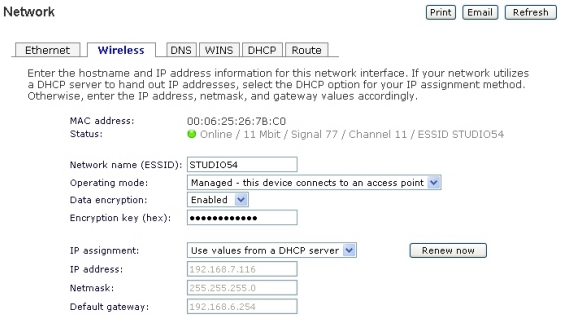
If you assign static IP addresses, beware that the browser will lose connection to the TeraNAS device after the IP address has been changed. You can click **Rescan** in RAIDar to rediscover the device and reconnect from there.

If your TeraNAS device comes with multiple Ethernet interfaces, you will see a separate configuration tab for each one.

Wireless

There are a couple of ways in which you can use this NAS device over wireless networking. You can either connect the NAS to your wireless access point with a Cat-5 Ethernet cable, or you can connect a USB wireless adapter directly to the NAS device and avoid the cabling.

The wireless network tab shows up in the Network menu when a supported USB wireless adapter is connected. Enter the **network name** (ESSID), **operating mode** (typically Managed if you have an access point), **data encryption mode**, and **encryption key values** from your wireless access point. Select the desired IP assignment method (DHCP or static) and save changes to start using your Tera NAS device over the wireless adapter.



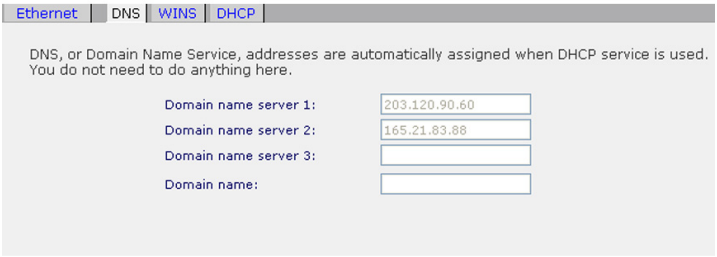
Note

Please note that support for USB wireless device is limited. Consult the hardware device compatibility list for a list of devices that is supported now. Future updates will support for more adapters.

DNS

The **DNS** tab allows you to specify up to three Domain Name Service servers for host name resolution. If you are unfamiliar with DNS, the service essentially translates host names into IP addresses.

DNS

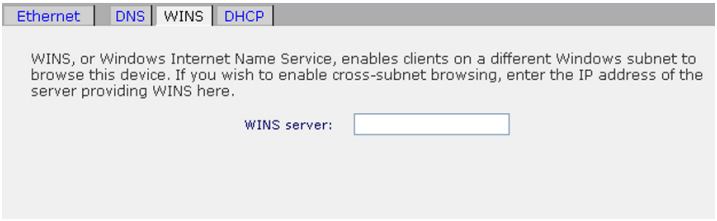


If you had selected the DHCP option in the Ethernet or Wireless tab, the domain name server fields will be automatically filled with the DNS settings from your DHCP server. If you had selected the Static option, you can manually specify the IP addresses of the DNS servers and the domain here.

WINS

The **WINS** tab allows you to specify the IP address of the WINS (Windows Internet Naming Service) server. A WINS server is typically a Windows server on the network that will allow the TeraNAS to be browsable from other subnets. Leave this blank if you are unsure.

Network


Ethernet
DNS
WINS
DHCP
WINS, or Windows Internet Name Service, enables clients on a different Windows subnet to browse this device. If you wish to enable cross-subnet browsing, enter the IP address of the server providing WINS here.
WINS server:

DHCP

The **DHCP** tab allows this device to act as a DHCP (Dynamic Host Configuration Protocol) server. DHCP service simplifies management of a network by dynamically assigning IP addresses to new clients on the network.

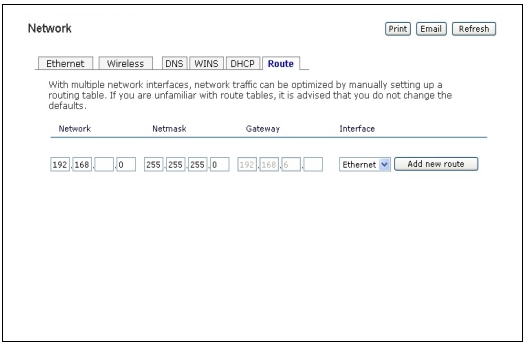
Click on the **Enable DHCP service** checkbox if you want the TeraNAS device to act as a DHCP server. This is convenient in networks where DHCP service is not already available.

Note

The options listed are available only if this device is not already using a DHCP address. Enabling DHCP service on a network already utilizing a DHCP server will introduce conflicts. If you wish to use this device as a DHCP server, make sure to specify static addresses in the Ethernet and DNS tabs.

Route

The **Route** tab is available if you have two or more network interfaces (Ethernet or Wireless combined) on your TeraNAS. In some environments, you can optimize your network traffic by manually setting up a routing table.

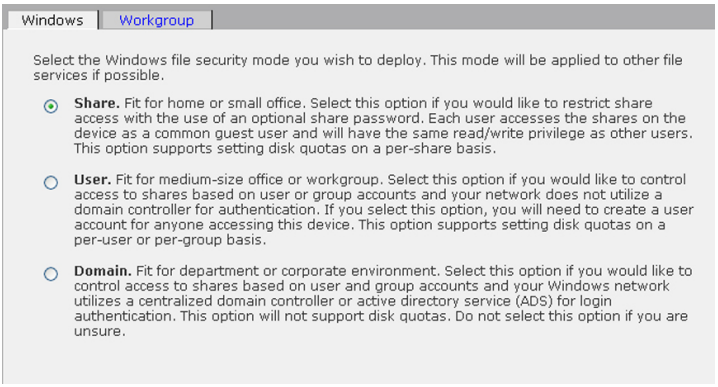


Route table management is beyond the scope of this manual, and this option is provided only for advanced users who understand routing and wish to deviate from the default routes.

Security

The TeraNAS device offers three security options for your network environment. Read the quick overview below and select the most appropriate one based on the level of security and how your current network authentication is implemented.

Shares


Windows
Workgroup
Select the Windows file security mode you wish to deploy. This mode will be applied to other file services if possible.
Share. Fit for home or small office. Select this option if you would like to restrict share access with the use of an optional share password. Each user accesses the shares on the device as a common guest user and will have the same read/write privilege as other users. This option supports setting disk quotas on a per-share basis.
User. Fit for medium-size office or workgroup. Select this option if you would like to control access to shares based on user or group accounts and your network does not utilize a domain controller for authentication. If you select this option, you will need to create a user account for anyone accessing this device. This option supports setting disk quotas on a per-user or per-group basis.
Domain. Fit for department or corporate environment. Select this option if you would like to control access to shares based on user and group accounts and your Windows network utilizes a centralized domain controller or active directory service (ADS) for login authentication. This option will not support disk quotas. Do not select this option if you are unsure.

The **Share** security mode fits the typical home and small office environments, providing a simple way for most people in a trusted environment to share files without the necessity for setting up separate user and group accounts. Shares that you create in this environment can be password-restricted if desired.

A more appropriate selection for the medium-size office or workgroup environment is the **User** security mode. This mode allows you to set up user and group accounts to allow for stricter share access restrictions. Access to shares require proper login authentication, and you can specify which users and/or groups you wish to offer access. As an example, you may want to restrict company financial data to just a few people or people belonging to one particular group. In this security

mode, the administrator will need to set up and maintain user and group accounts on the TeraNAS device. Each user will be set up with a private home share on the TeraNAS.

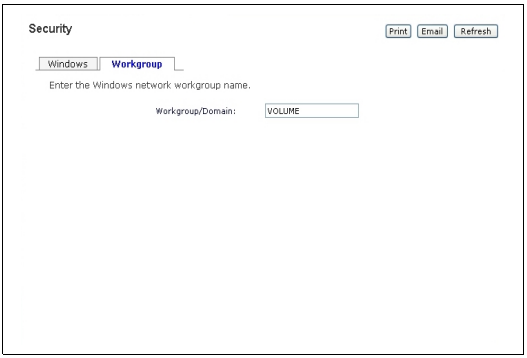
The **Domain** security mode is appropriate for the larger department or corporate environment, where a centralized Windows-based domain controller or active directory server is present. The TeraNAS device easily works in this environment by creating a trusted relationship with the domain/ADS authentication server and allowing all user authentications to occur there, eliminating the need for account administration on the device itself. Also, in this security mode, each domain/ADS user will be set up with a private home share on the TeraNAS.

Share Mode

The **Share security mode** is the simplest security option to set up. You only need to specify a workgroup if you wish to change it from default.

SPECIFY A WORKGROUP

To change the workgroup name, click on the **Workgroup** tab and enter a new name.



A valid workgroup name must conform to the following restrictions:

- Name must consist of characters a-z, A-Z, 0-9, and the symbols _ (underscore), – (dash), and . (period).
- Name must start with a letter.
- Name length must be 15 characters or less.

User Mode

In **User security mode**, you will specify a workgroup name just as you would in the previous security option, and create user and group accounts. You will have control over how much disk space is allocated for each user or group.

In this security mode, each user will be given a home share on the TeraNAS device that the user can use to keep private data such as backups of the user's PC. This private share is accessible only by that user and the admin user who needs the privilege to perform backups of these private shares.

Note

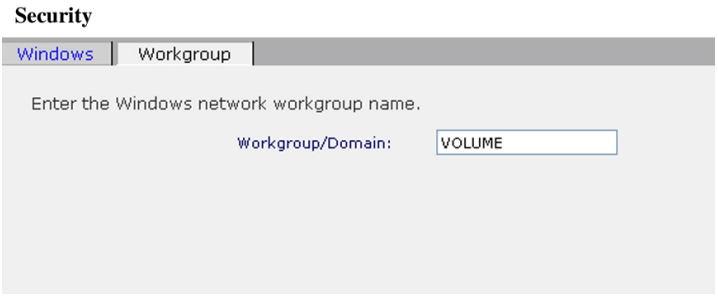
Private user shares are only accessible by users using CIFS (Windows) or AppleTalk file protocols.

To set up the TeraNAS for this security mode, you will need the following information:

- Workgroup name
- Group names you wish to create (i.e. Marketing, Sales, Engineering)
- User names you wish to create (plus email addresses if you will be setting disk quotas)
- Amount of disk space you would like to allocate to users and groups (optional)

SPECIFY A WORKGROUP

To specify a workgroup name, click on the Workgroup tab and enter the name. The name can be the workgroup name that is already used on your Windows network.



SETTING UP ACCOUNTS

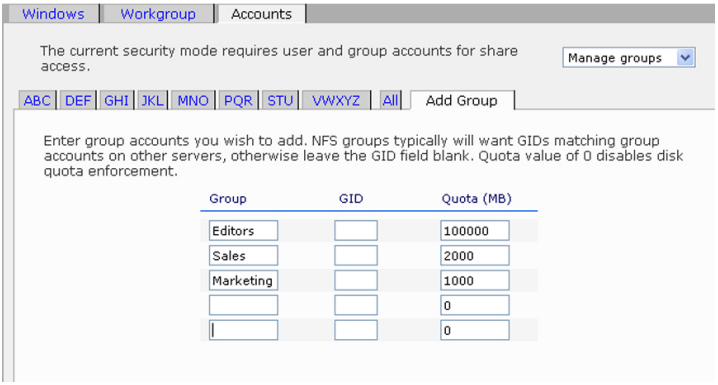
In this security mode, the Accounts tab is available where you can manage user and group accounts on the TeraNAS device. A good starting point would be to select the **Manage groups** option from the selection box in the upper right corner.

MANAGING GROUPS

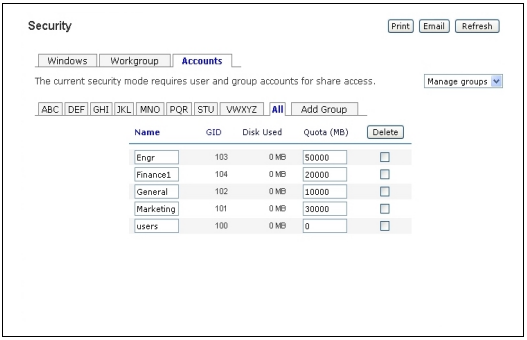
To add a new group, click on the **Add Group** tab if it is not already selected. You can add up to five groups at a time. If you expect to have just one big set of users for one group, you can forego adding a new group and accept the default **users** group.

While adding a new group, you can specify the amount of disk space you wish to allocate that group by setting disk quota. A value of **0** denotes no limit. You can set or change the quota at a later time. You can also set the Group ID, or GID, of the group that you are adding. You can leave this field blank and let the system automatically assign this value unless you wish to match your GID to your NFS clients.

Security



After adding your groups, you can view or change your groups by clicking on the alphabetical index tab, or **All** to list all groups.



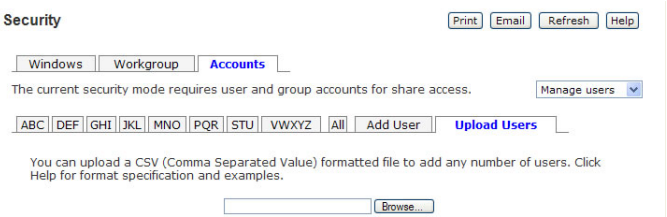
MANAGING USERS

To manage user accounts, select the **Manage users** option.

To add a user, click on the **Add User** tab. You can add up to five users at a time.

Enter a user name, email address, user ID, select a group, password, and disk quota for the user. Only the user name and password fields are required, however, you should specify the user email address if you intend to set up disk quotas. Without an email address, the user will not be warned when disk usage approaches the specified disk quota limit. If you do not wish to assign a disk quota, enter **0**.

If you wish to add a large number of users, click on the **Upload Users** tab.



Here, you can upload a CSV (Comma Separated Value) formatted file containing the user account information. The format of the file is:

```
name1,password1,group1,email1,uid1,quota1
name2,password2,group2,email2,uid2,quota2
name3,password3,group3,email3,uid3,quota3
                    :
```

Please note the following:

- Spaces around commas are ignored.
- The name and password fields are required.
- Password must be 1 to 8 characters in length.
- If a listed group account does not exist, it will be automatically created.
- Group and quota will be set to the defaults if not specified.
- Email notification will not be sent to the user if the field is ommitted or left blank.
- UID will be automatically generated if not specified.

- Empty fields are replaced with accounts defaults.

Examples of acceptable formats are as follows (note that you can ommit follow-on commas and fields if you wish to accept the system defaults for those fields, or you can leave the fields empty):

```
fred,hello123
```

In this example, user **fred** will have password set to *hello123*, belongs to the default group, no email notification, automatic UID assigned, and default quota.

```
barney,23stone,,barney@bedrock.com
```

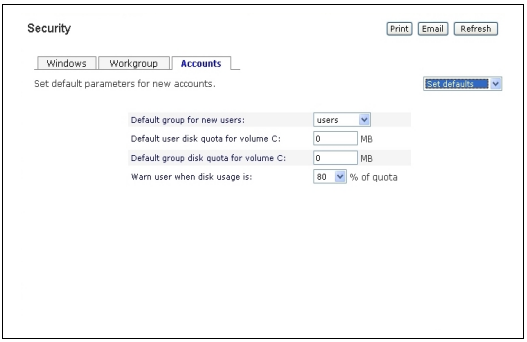
In this example, user **barney** will have password set to *23stone*, belongs to the default group, will be sent email notification to *barney@bedrock.com*, automatic UID assigned, and default quota.

```
wilma,imhiswif,ourgroup,wilma@bedrock.com,225,50
```

In this example, user **wilma** will have password *imhiswif*, belongs to group *ourgroup*, email notification sent to *wilma@bedrock.com*, UID set to *225*, and quota set to *50MB*.

SETTING ACCOUNTS DEFAULTS

You can set accounts default by selecting the **Set defaults** option. Here you can set up default group for new users, default user and disk quotas, and default warning point when email alerts should be sent to users approaching quota limits. If multiple volumes are configured, you can select which volume the user private home share will reside.

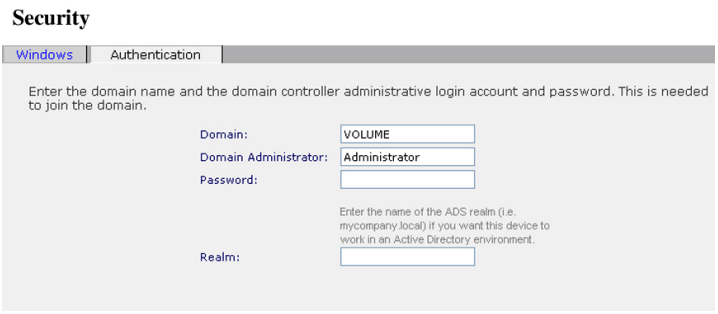


Domain Mode

DOMAIN/ADS AUTHENTICATION

If you choose the **Domain security mode** option, you will need to create a trusted relationship with the domain controller or the active directory server (ADS) that will act as the authentication server for the TeraNAS device. You will need the following information:

- Domain name
- Domain administrator login
- Domain administrator password
- DNS name of the ADS realm (if using ADS)


Security
Windows
Authentication
Enter the domain name and the domain controller administrative login account and password. This is needed to join the domain.
Domain:
VOLUME
Domain Administrator:
Administrator
Password:
Enter the name of the ADS realm (i.e. mycompany.local) if you want this device to work in an Active Directory environment.
Realm:

Enter these items in the Authentication tab and click Apply. If successful, the TeraNAS device will have joined in the domain and all users and groups from the domain will have login access to the shares on this device.

Shares

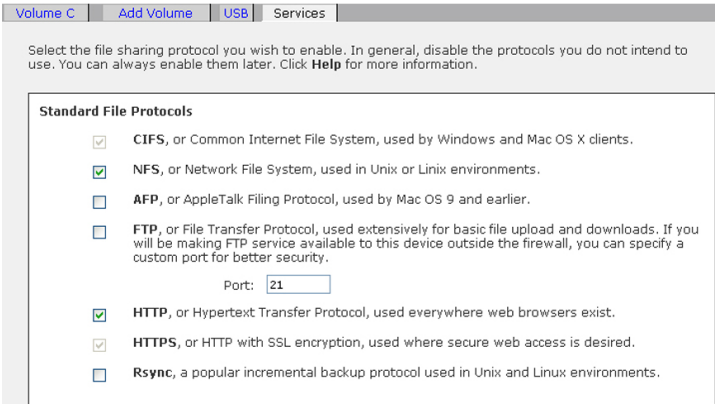
The Shares menu provides all the options pertaining to share services for the TeraNAS clients. This entails share management (including data and print shares), volume management, and share service management.

We'll first look at how we can control the services.

Services

The **Services** tab allows you to manage the file protocols for share access. This in effect controls the type of clients you wish to enable share access.

Shares


Volume C
Add Volume
USB
Services
Select the file sharing protocol you wish to enable. In general, disable the protocols you do not intend to use. You can always enable them later. Click Help for more information.
Standard File Protocols
CIFS, or Common Internet File System, used by Windows and Mac OS X clients.
NFS, or Network File System, used in Unix or Linix environments.
AFP, or AppleTalk Filing Protocol, used by Mac OS 9 and earlier.
FTP, or File Transfer Protocol, used extensively for basic file upload and downloads. If you will be making FTP service available to this device outside the firewall, you can specify a custom port for better security.
Port: 21
HTTP, or Hypertext Transfer Protocol, used everywhere web browsers exist.
HTTPS, or HTTP with SSL encryption, used where secure web access is desired.
Rsync, a popular incremental backup protocol used in Unix and Linux environments.

The file protocols are a bunch of daunting acronyms if you are not accustom to them, but we'll try to decipher them for you here.

- **CIFS**, or Common Internet File Service. This protocol is used by Microsoft Windows and Mac OS X clients. Under Windows, when you click on My Network Places or Network

Neighborhood, you're going across CIFS. This service is enabled by default and cannot be disabled.

- **NFS**, or Network File Service. NFS is used by Linux and Unix clients. Mac OS 9/X users can access NFS shares as well through console shell access.
- **AFP**, or AppleTalk File Protocol. Mac OS 9 uses this protocol. Mac OS X supports this but it now defaults to using CIFS.
- **FTP**, or File Transfer Protocol. Widely used in public file upload and download sites. TeraNAS supports anonymous access for FTP clients.
- **HTTP**, or Hypertext Transfer Protocol. Used by web browsers. TeraNAS supports HTTP file manager, allowing web browsers to read and write to shares using the web browser. This service can be disabled in leiu of HTTPS to allow for a more secure transmission of passwords and data.
- **HTTPS**, or HTTP with SSL encryption. This service is enabled by default and cannot be disabled. Access to FrontView is strictly through HTTPS for this reason.

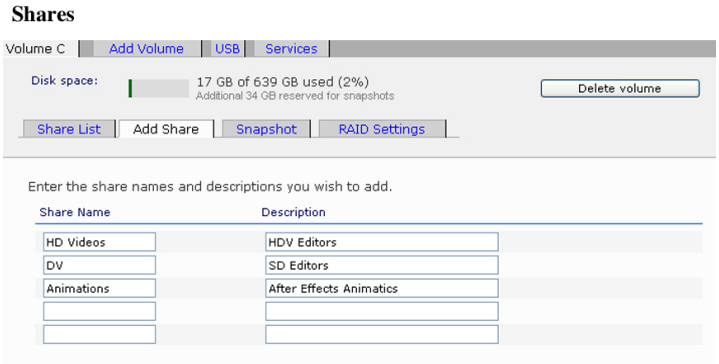
Enable the services to wish to support and disable the ones you will not be using.

Adding Shares

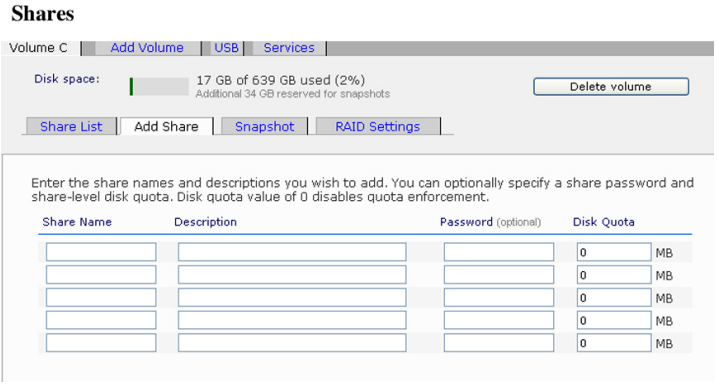
To add a share, click on the Volume tab. If more than one volume is configured, click on the volume you wish to add the share.

The **Add Share** tab has two looks, depending on the security mode. In the **Share** mode, you will enter the share name, description, and

optional password and disk quota. The share password and share disk quota is available only in this security mode.



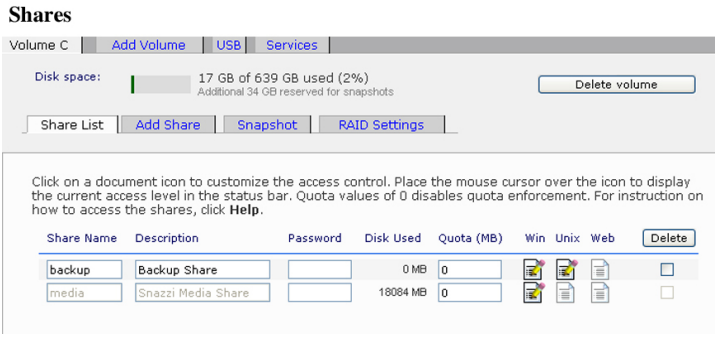
In the **User** or **Domain** security modes, the **Add Share** tab consists only of fields for the share name and description. Password and disk quotas are account-specific.



In either case, you can add up to five shares at a time. Once you finish adding the shares, you can refer to Chapter 2 for instructions on how to access them from different client interfaces.

Managing Shares

Once you have added shares, you may want to manually fine-tune share access in the **Share List** tab. This tab has two looks, one for **Share** security mode and one for **User** and **Domain** mode. They're both similar except for the password and disk quota prompts which only appear in Share mode.



If you want to delete a share, click on the checkbox to the far right of the share listing and click **Delete**. You have the option of deleting up to five shares at a time.

The columns to the left of the Delete checkbox represent the services that are currently enabled, and the access icons in those columns summarize the access rights to the share for each of the services. You can hover the mouse pointer over the access icons to get a quick glimpse of the access settings.

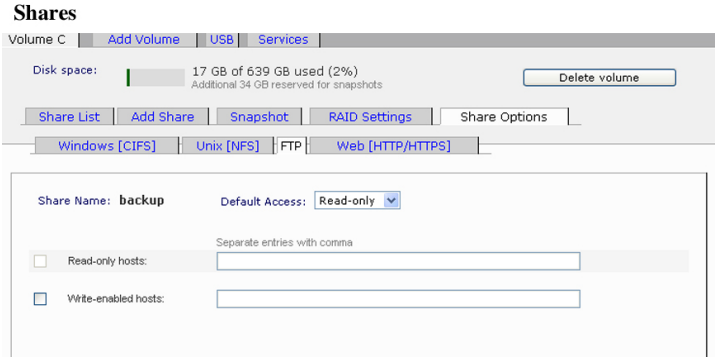
The settings represent:

- **Disabled** – Access to this share is disabled.
- **Read-only Access** – Access to this share is read-only.
- **Read/Write Access** – Access to this share is read/write.
- **Read Access with exceptions** – Either (1) access to this share is read-only and only allowed for specified hosts, (2) access is read-only except for one or more users or groups that are granted read/write permission, or (3) access is disabled except for one or more users or groups that are granted read-only privilege.
- **Write Access with exceptions** – Either (1) access to this share is read/write and only allowed for specified hosts, (2) access is read/write except for one or more users or groups that are restricted to read-only access, or (3) access is disabled except for one or more users or groups that are granted read/write privilege.

You can click on the access icon to bring up the Share Options tab where you can set the access rules for each file protocol. Keep in mind that access specification will differ between protocols.

SETTING SHARE ACCESS IN SHARE MODE

In Share mode, the CIFS/Windows share options tab looks as follows:



In this tab, you can select the default access at the top and specify the host(s) that you wish to allow. For instance, select **read-only** for default access and list the hosts you wish to allow access to. Access from all other hosts will be denied. For example, to allow only host *192.168.2.101* read-only access to the share, specify the following:

```
Default:                Read-only
Hosts allowed access:   192.168.2.101
```

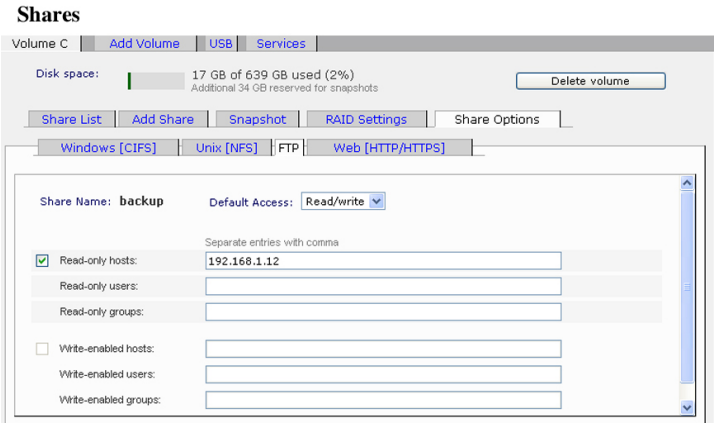
Multiple hosts can be separated with commas (see **Appendix B** for more description of valid host formats.) For example, if you wish to limit access to the share to particular hosts, you can enter host IP addresses or valid DNS hostnames in the **Host allowed access** field. In addition, you can enter a range of hosts using common IP range expressions such as:

```
192.168.2., 192.168.2.0/255.255.255.0, 192.168.2.0/8
```

The above designations all allow hosts with IP addresses *192.168.2.1* through *192.168.2.254*.

SETTING SHARE ACCESS IN USER AND DOMAIN MODES

In User or Domain modes, the same tab would look as follows (note the addition of read-only and write-enabled user and group fields):



If you wish to limit share access to particular users and/or groups, you can enter their names in the **Read-only users**, **Read-only groups**, **Write-enabled users**, and **Write-enabled group** fields. The names must be valid accounts, either on the TeraNAS or on the domain controller.

For instance, if you wish to allow read-only access to all and read/write access only user *fred* and group *engr*, you would set the following:

```
Default:                Read-only
Write-enabled users:    fred
Write-enabled groups:   engr
```

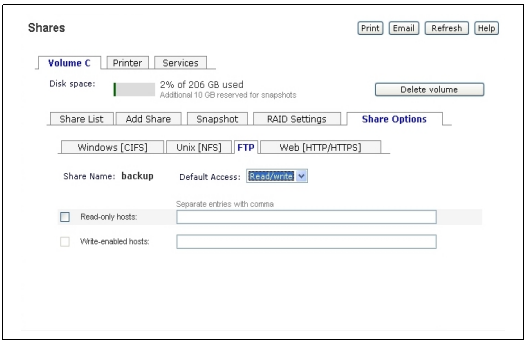
If you wish to limit the above access only to hosts *192.168.2.101* and *192.168.2.102*, set the following:

```
Default:                Read-only
Hosts allowed access:   192.168.2.101,
192.168.2.102
Write-enabled users:    fred
Write-enabled groups:   engr
```

If you wish to specify some users and groups for read-only access and some for read/write access, and disallow all other users and groups, enter the following:

```
Default:                Disabled
Hosts allowed access:   192.168.2.101,
192.168.2.102
Read-only users:        mary, joe
Read-only groups:       marketing, finance
Write-enabled users:    fred
Write-enabled groups:   engr
```

Note that access control will differ slightly from service to service. For instance, FTP tab will have **Read-only hosts** and **Write-enabled hosts**, but no user and group access control options.



Taking and Scheduling Snapshot

The Volume page offers the ability to schedule and take snapshots. You can visualize a snapshot as a frozen image of a volume at the time you take the snapshot. Snapshots are typically used for backups during which time the original volume can continue to operate normally. As primary storage becomes larger, offline backups tend to become increasing difficult as backup time increases beyond offline hours. Snapshots allow backups to occur without taking systems offline.

Snapshots also can be used as temporary backups as well, perhaps as a means to backup data against viruses. As an example, if users detect a virus attack on files on the NAS device, files can be restored from a prior snapshot taken before the attack.

To take or schedule a snapshot, click on the **Snapshot** tab.

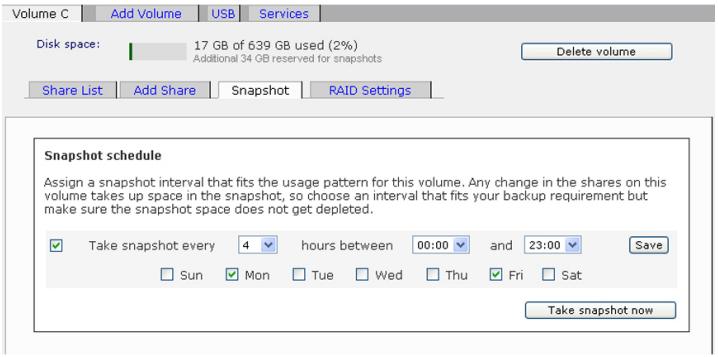
Note

If you do not see a Snapshot tab within your volume tab, you did not reserve any space for snapshots when you added the volume. TeraNAS ships with a snapshot reserved space of 5% for volume C.

In the tab, you can specify how often a snapshot should be taken and on which days. Snapshots can be scheduled from once every 4 hours to once a week.

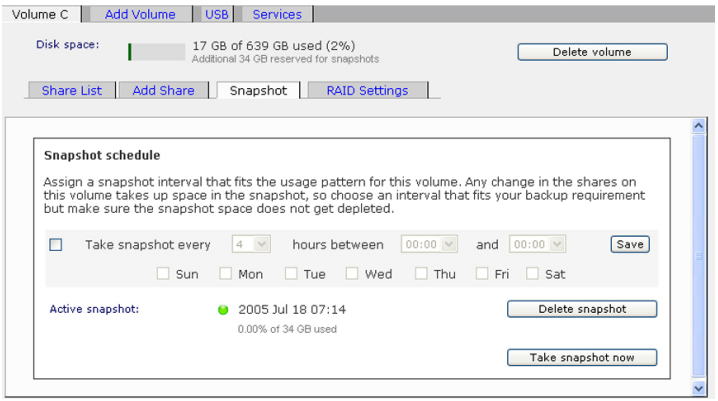
Specify the frequency and the days that you wish to schedule a snapshot. A start and end-time of 00:00 will take one snapshot at midnight. A start time of 00:00 and end-time of 23:00 will take snapshots between midnight and 11pm the next day at the interval you specify. Once you save the snapshot schedule, the time of the next snapshot will be displayed. When the next snapshot is taken, the previous one is deleted.

Shares

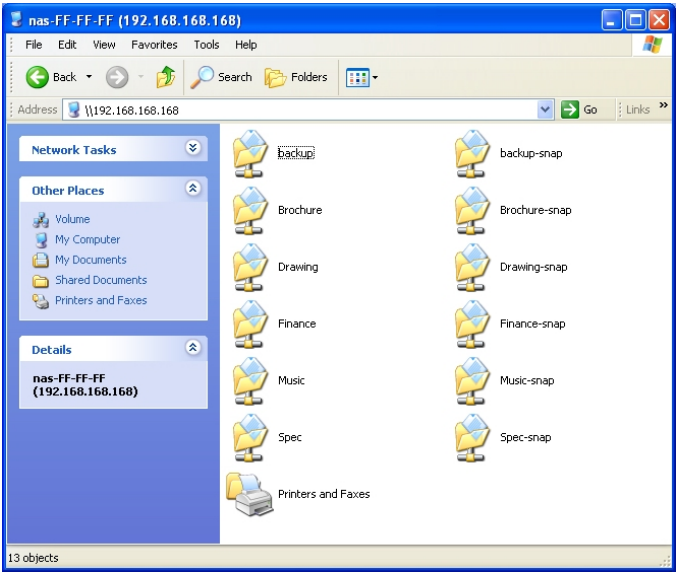


If you prefer, you can manually take a snapshot – just click on **Take snapshot now**.

Shares

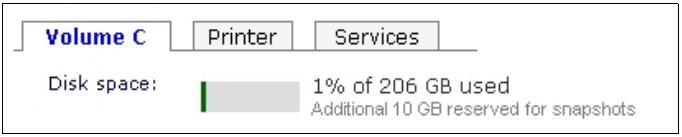


When a snapshot is taken, snapshots of shares appear in your browse list alongside the original shares, except the snapshot share names have *–snap* appended to the original share names. For example, a snapshot taken of share **backup** will be available as **backup-snap**.



You can traverse a snapshot share just as you would a normal share except that the snapshot share is read-only. If you wish, you can select a detailed listing to show the snapshot time in the description field.

Do note that snapshots can expire when the snapshot reserved space is filled. The snapshot mechanism keeps track of data that has been changed from the original volume starting at the point when the snapshot is taken. All these changes are kept in the snapshot reserved space on the volume. If you look at the **Disk space** utilization information just below the **Volume** tab, you will see how much space has been reserved for snapshots.



From the point when the snapshot is taken, if changes on the volume exceed this reserved space, the snapshot is invalidated and can no longer be used.

Note

Changes that takes up space in the snapshot reserved space include new file creation, modifications, and deletions; for instance, any time you delete a 1MB file, the change caused by the deletion will use up 1MB of reserved space.

When the snapshot does become invalidated, an email alert will be sent and the status will be reflected in the **Snapshot** tab. If you are constantly getting this notification, you may want to either increase the frequency of the snapshot, or consider re-creating the volume with a larger snapshot reserved space. This is covered in the next section.

Note

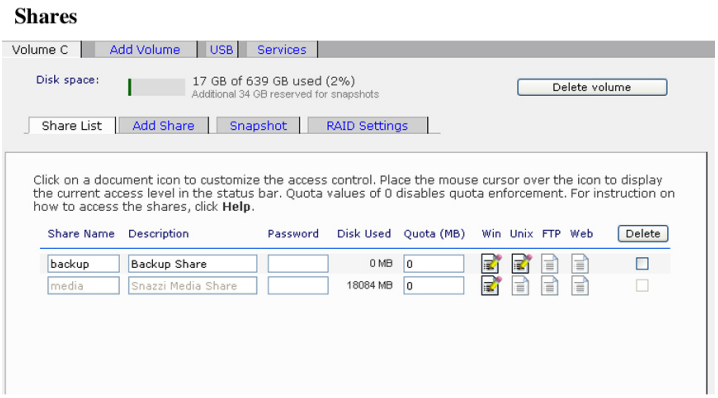
Due to the nature of how snapshots work, you will encounter a drop in write performance when a snapshot is active. If your environment requires the highest throughput in performance, the active snapshot should be deleted and any snapshot schedule should be disabled.

Volume Management

If you wish to reconfigure the default volume C, wish to split it into multiple volumes, specify a different RAID level, or specify a larger reserved space for snapshots, you will need to reconfigure your volume. The first step is to delete the existing volume you wish to replace.

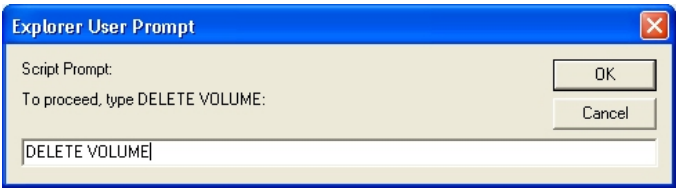
DELETING A VOLUME

To delete a volume, click on the volume tab of the volume you wish to delete, or Volume C if only one volume is configured. Make sure if you have data in that volume that you back up the files you wish to keep first. All shares, files, and snapshots residing on that volume will be deleted and are non-recoverable.



Click **Delete Volume** in the Volume C tab.

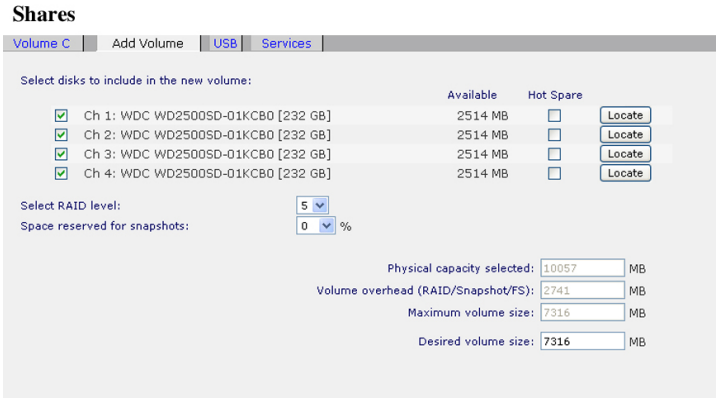
You will be asked to confirm your intention by typing: **DELETE VOLUME**



ADDING A VOLUME

You will then be presented with the **Add Volume** tab listing the available configurable space on the hard disks. All the disks will be selected by default. You can elect to specify a hot spare disk if you wish. A hot spare remains in standby mode and will automatically regenerate the data from a failed disk from the volume. A hot spare disk is only available for RAID level 1 and RAID level 5 if there is enough disks to fulfill the minimum required plus one.

Select Hard Disks



In our example here, we'll select the first three disks and elect not to specify any of them as a hot spare.

Select RAID level

RAID level determines how the redundancy, capacity utilization, and performance is implemented for the volume. See Appendix A, "RAID Levels Simplified", for more information. Typically in a three or more disk configuration, RAID level 5 is recommended.

In our example above, we selected RAID level 5 for the three selected disks.

Specify reserve space for snapshot

Next, select the percentage of the volume you wish to allocate for snapshots. You can elect to specify 0 if you wish to disable snapshot capability, or you can specify a percentage in 5% increment from 5 to 50%.

The percentage represents the amount of data you feel would be changing while the snapshot is active. This typically depends on how often you schedule your snapshot (see previous section on snapshot), and the maximum amount of data (plus padding) you feel will change

during that time. Make sure to allocate enough space for worse case as the snapshot becomes unusable when its reserved space runs out.

In our example above, we selected 10% of the volume to be reserved for snapshots.

Note

If you do not reserve any space for snapshot, the snapshot tab will not display within the volume tab.

Specify desired volume size

After you've specified the above volume parameters, enter the desired volume size if you wish to configure a smaller volume size than the maximum displayed. The resulting volume will be approximately the size that is specified.

In our example above, we kept the maximum size that was calculated.

Click **Apply** and wait for instruction to reboot the system. It typically takes about a minute before you are notified to reboot.

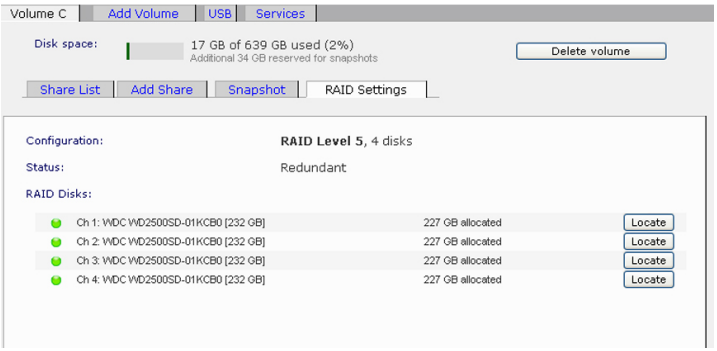
After rebooting, you will then be notified by email when the volume has been added. Use RAIDar to reconnect to the NAS device.

RAID SETTINGS

After you have added a volume, you can revisit the Volume tab and click on the **RAID Settings** tab to display the current RAID information and configuration options for the volume.

Notice the disk on channel 4 that we did not configure is listed in the Available Disks section. We can add this disk as a hot spare by clicking on the **Make hot spare** button.

Shares



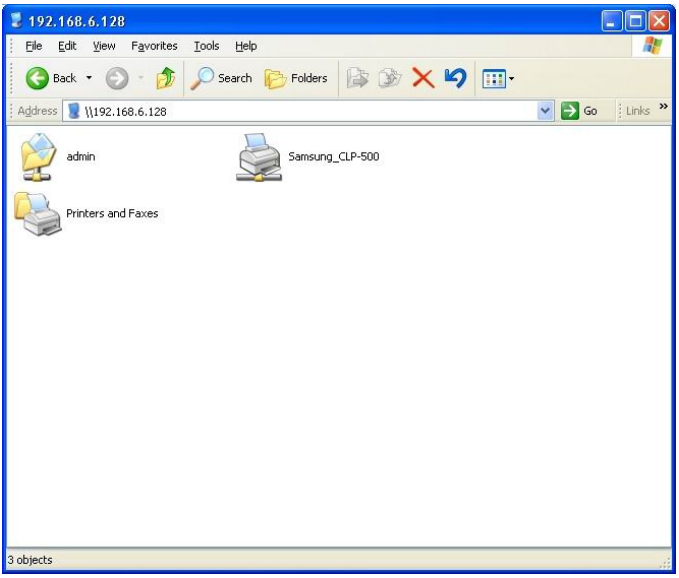
We can also remove a disk from the volume by clicking on the **Remove** button. The Remove operation is a maintenance feature and is not a recommended in a live environment. Its function is equivalent to hot-removing the disk or simulating a disk failure. The volume will still be available but in a non-redundant state. An additional disk failure would render this volume unusable.

The **Locate** option is available as a way to verify that a disk is correctly situated in the expected disk slot. Clicking on **Locate** will blink the LED of the disk for 15 seconds.

Printers

The TeraNAS device supports automatic recognition of USB printers. If you have not already done so, you can connect a printer now, wait a few seconds, and click on the Printer tab or **Refresh** on that page to display it in the list. The print share name will automatically reflect the manufacturer and model of your printer and will appear in the Printer tab.

TeraNAS will act as a print server to up to two USB printers for your Windows clients. You can click Browse in RAIDar or simply enter **\\hostname** in the Explorer address bar to list all data and printer shares on the TeraNAS.

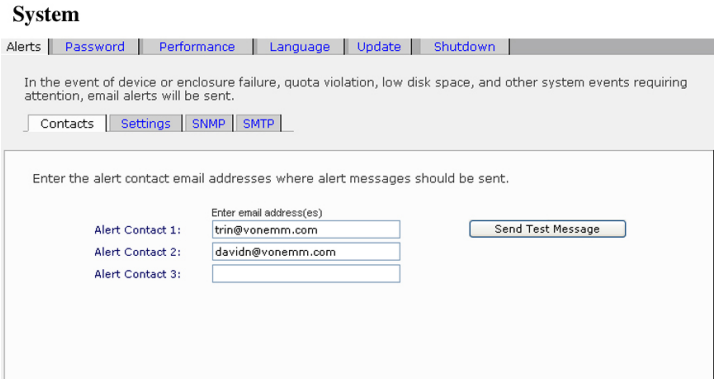


Double-click the printer icon to assign a Windows driver.

Alerts

ALERTS CONTACTS

The **Contacts** tab allows you to specify up to three email addresses where system alerts will be sent. The TeraNAS device is pretty adamant about communicating with you if something appears wrong or perhaps a device has failed. The best way to do this is with an email alert system. Make sure to enter a primary email address and a secondary one if possible.

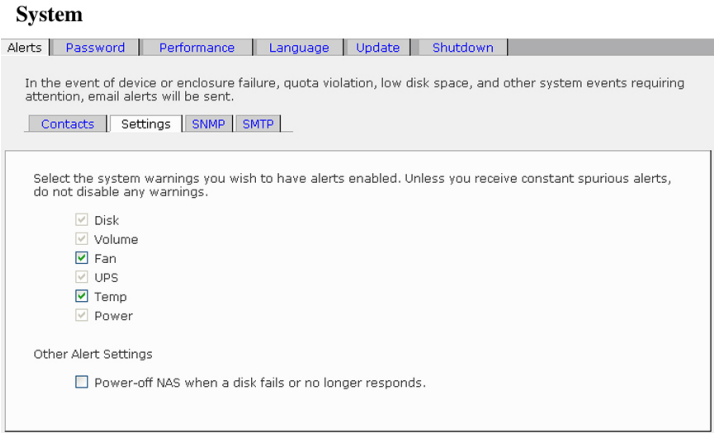


Some email addresses can be tied to a mobile phone, and this is a great way to monitor the device when you might be away from your normal email access.

ALERTS SETTINGS

This TeraNAS device has been pre-configured with mandatory and optional alerts for various system device warnings and failures. The

Alerts Settings tab allows you to control the settings for the optional alerts.

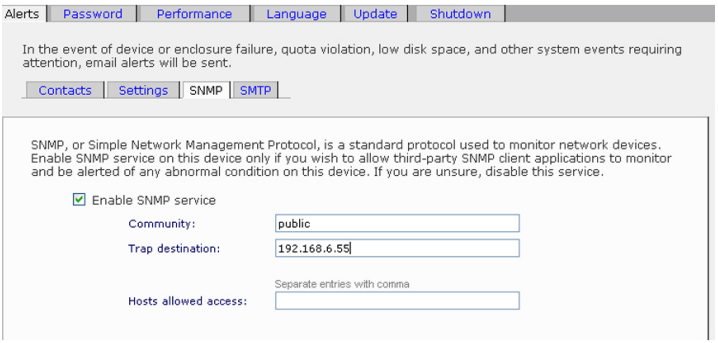


It is highly recommended that all alerts are kept enabled; however, you may choose to disable an alert if you are aware of a problem and wish to disable the constant alert messages.

SNMP

If you utilize a SNMP management system such as HP OpenView or CA Unicenter to monitor devices on your network, you can set up the TeraNAS device to work within this infrastructure.

System


Alerts
Password
Performance
Language
Update
Shutdown
In the event of device or enclosure failure, quota violation, low disk space, and other system events requiring attention, email alerts will be sent.
Contacts
Settings
SNMP
SMTP
SNMP, or Simple Network Management Protocol, is a standard protocol used to monitor network devices. Enable SNMP service on this device only if you wish to allow third-party SNMP client applications to monitor and be alerted of any abnormal condition on this device. If you are unsure, disable this service.
Enable SNMP service
Community:
public
Trap destination:
192.168.6.55
Separate entries with comma
Hosts allowed access:

To set up SNMP service, check the **Enable SNMP service** checkbox in the **SNMP** tab. You can leave the **Community name** as *public*, or specify a private name if you have opted for a more segregated monitoring scheme.

Next, enter a host name or an IP address for **Trap destination**. This is where all trap messages will be sent. The following system events will generate a trap:

- Abnormal power voltage
- Abnormal board enclosure temperature
- Fan failure
- UPS connected
- UPS detected power failure
- RAID disk sync started and finished
- RAID disk added, removed, and failure
- Snapshot invalidated

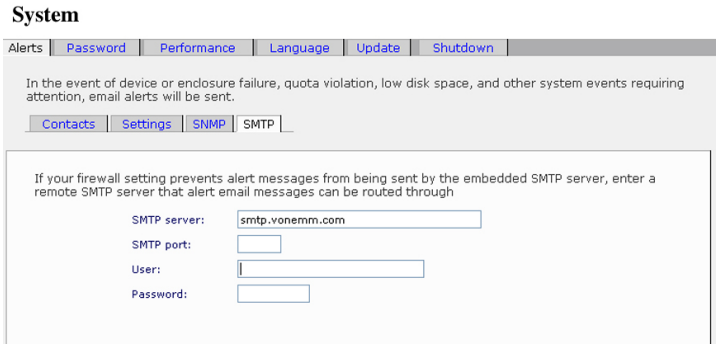
If you wish to limit SNMP access to only a secure list of hosts, you list the hosts in the **Hosts allowed access** field.

When you have saved the SNMP settings on the TeraNAS, you can import the Infrant SNMP MIB to your SNMP client application. The Infrant MIB can be obtained from the included Installation CD-ROM or downloaded from the Infrant Support site at http://www.infrant.com.

SMTP

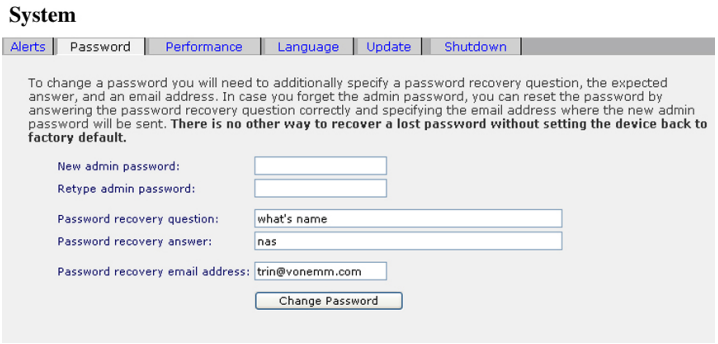
The TeraNAS device has a built-in email message transfer agent (MTA) and is set up automatically to allow information and alert email messages to be sent out from the device. Some corporate environments however have adopted a firewall that blocks untrusted MTA from sending out messages.

If you were unable to receive the test message from the **Alerts Settings** tab, it may have been blocked by the firewall. In that case, specify the your SMTP server in this tab.



Admin Password

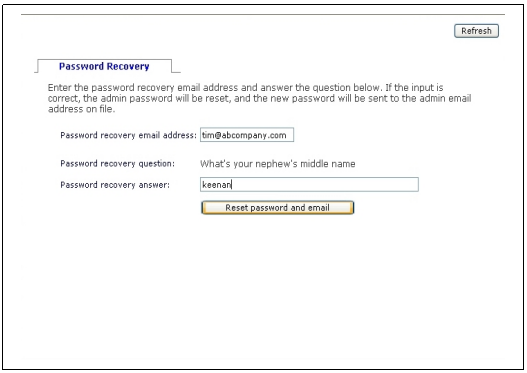
The **Password** tab allows you to change the **admin** user password. Be sure to set a password different from the default password and make sure this password is kept in a safe place. Anyone who obtains this password can effectively wipe out your data on the TeraNAS.


System
Alerts
Password
Performance
Language
Update
Shutdown
To change a password you will need to additionally specify a password recovery question, the expected answer, and an email address. In case you forget the admin password, you can reset the password by answering the password recovery question correctly and specifying the email address where the new admin password will be sent. There is no other way to recover a lost password without setting the device back to factory default.
New admin password:
Retype admin password:
Password recovery question:
what's name
Password recovery answer:
nas
Password recovery email address:
trin@vonemm.com
Change Password

Note

In User or Domain security mode, you can use the **admin** account to login to a Windows share, and perform maintenance on any file or folder in that share. The admin user also has permission to access all user private home shares to perform backups.

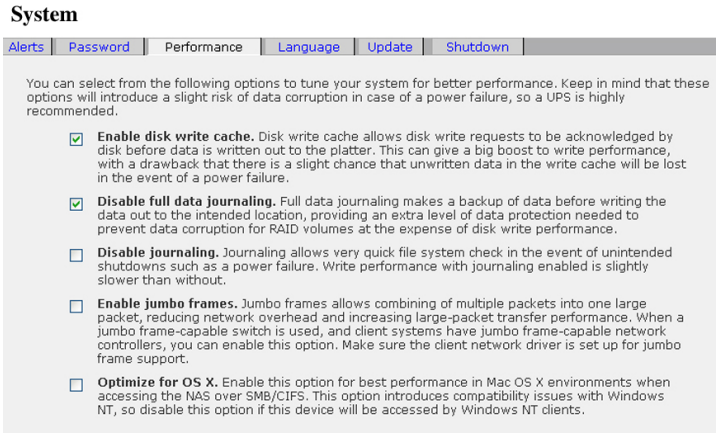
As a safeguard, you will be requested to enter a password recovery question, the expected answer, and an email address. If, in the future, you forget the password, you can go to https://*ip_address*/password_recovery. Successfully answering the questions there will reset the admin password, and that new password will be sent to the email address you enter in this tab.


Refresh
Password Recovery
Enter the password recovery email address and answer the question below. If the input is correct, the admin password will be reset, and the new password will be sent to the admin email address on file.
Password recovery email address:
tim@abcompany.com
Password recovery question:
What's your nephew's middle name
Password recovery answer:
keenan
Reset password and email

Performance

If you wish to tweak the system performance, select the **Performance** tab in the **System** menu. TeraNAS ships with conservative system defaults that meant to provide the utmost protection of your data. If you do utilize a UPS (Uninterruptible Power Supply) or your application requires a more aggressive approach to performance, you can select one of more of the available options here.

Select **Enable disk write cache** if you want to utilize the performance advantages of write caching on the hard disks. For utmost protection of data, you should utilize a UPS to back up the write cache in case of power failure; otherwise, there is a slight chance that data queued up in the cache will be lost.


System
Alerts
Password
Performance
Language
Update
Shutdown
You can select from the following options to tune your system for better performance. Keep in mind that these options will introduce a slight risk of data corruption in case of a power failure, so a UPS is highly recommended.
Enable disk write cache. Disk write cache allows disk write requests to be acknowledged by disk before data is written out to the platter. This can give a big boost to write performance, with a drawback that there is a slight chance that unwritten data in the write cache will be lost in the event of a power failure.
Disable full data journaling. Full data journaling makes a backup of data before writing the data out to the intended location, providing an extra level of data protection needed to prevent data corruption for RAID volumes at the expense of disk write performance.
Disable journaling. Journaling allows very quick file system check in the event of unintended shutdowns such as a power failure. Write performance with journaling enabled is slightly slower than without.
Enable jumbo frames. Jumbo frames allows combining of multiple packets into one large packet, reducing network overhead and increasing large-packet transfer performance. When a jumbo frame-capable switch is used, and client systems have jumbo frame-capable network controllers, you can enable this option. Make sure the client network driver is set up for jumbo frame support.
Optimize for OS X. Enable this option for best performance in Mac OS X environments when accessing the NAS over SMB/CIFS. This option introduces compatibility issues with Windows NT, so disable this option if this device will be accessed by Windows NT clients.

The **Disable full data journaling for RAID 5 volumes** option also should be selected only if the NAS has UPS protection. Without battery backup, there is a small chance that parity written to a disk in a RAID 5 set may become out of sync with the data disks if a power failure occurred, possibly causing incorrect data to be recovered if one disk fails. Without full data journaling, disk write performance can increase substantially.

Select **Disable journaling** if you understand the consequences of the 2nd option above, and you don't mind a long file system check after a power failure. File system journaling allows recovery time of a few seconds verses possibly an hour or longer without journaling. Disabling journaling may improve disk write performance slightly.

Note

You can buy a UPS with USB monitoring for less than $50 (US dollars). With more aggressive performance settings afforded by a UPS, you can effectively double your write performance and provide uninterrupted service of your TeraNAS for a very low price.

ADDING A UPS FOR PERFORMANCE

Adding a UPS to the NAS is a sure way to protect against power failures, but as mentioned in the **System Performance** section, a UPS can also allow for a more aggressive performance setting. Simply connect the NAS power cable to the UPS and connect the UPS USB monitoring cable between the UPS and the NAS[1]. The UPS will be detected automatically and will show up in the Status bar. You can hover the mouse pointer over the UPS LED icon to display the current UPS information and battery life.

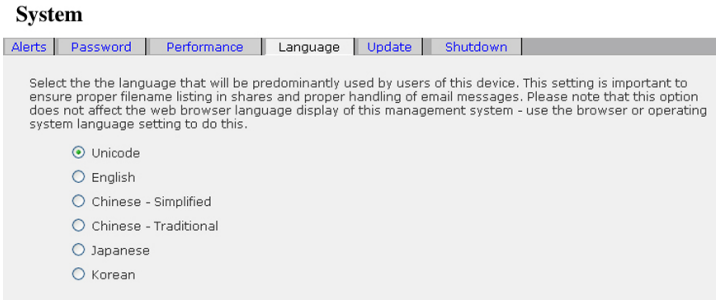
You will be notified by email whenever the status of the UPS changes, i.e. when a power failure forces the UPS to be in battery mode and when the battery is low. When the battery is low, the NAS device will automatically shutdown gracefully.

[1] Note that alert notification and automatic system optimization is available only with UPS utilizing a USB monitoring interface.

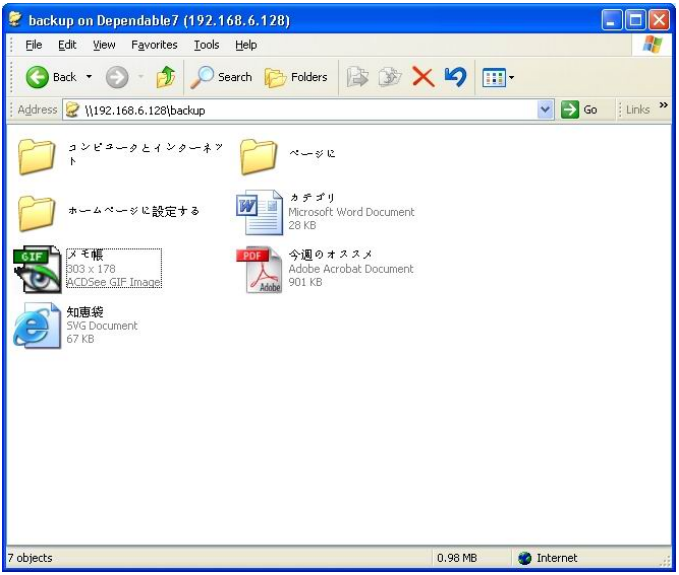
Make sure to adjust the optimization settings in the Performance tab if you wish to take advantage of the available options.

Language

The **Language** tab offers the option of setting the TeraNAS device to appropriate character set for file names when files are shared with non-unicode supported operating systems.


System
Alerts
Password
Performance
Language
Update
Shutdown
Select the the language that will be predominantly used by users of this device. This setting is important to ensure proper filename listing in shares and proper handling of email messages. Please note that this option does not affect the web browser language display of this management system - use the browser or operating system language setting to do this.
Unicode
English
Chinese - Simplified
Chinese - Traditional
Japanese
Korean

For example, selecting Japanese allows sharing of files with Japanese names in Windows Explorer.



It is best to select the appropriate language based on the region that this device will operate in.

Note

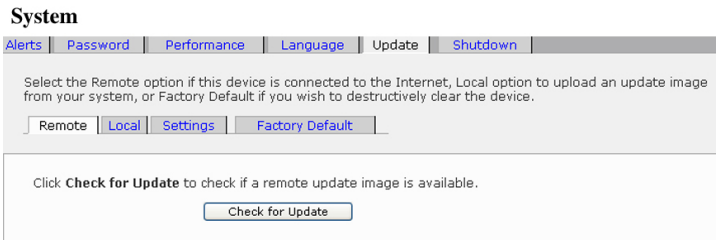
This option does not set the web browser language display – browser settings must be done using the browser language option.

Updating TeraNAS

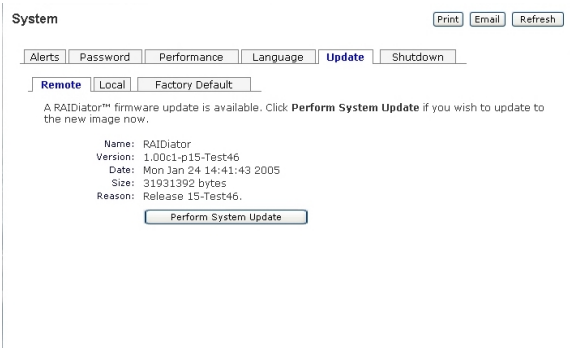
The TeraNAS device offers the option of upgrading the operating firmware either directly using the Remote Update option or reading in an update image downloaded from the Infrant Support website.

REMOTE UPDATE

The preferred and quicker method if you have Internet access is the **Remote** update option.


System
Alerts
Password
Performance
Language
Update
Shutdown
Select the Remote option if this device is connected to the Internet, Local option to upload an update image from your system, or Factory Default if you wish to destructively clear the device.
Remote
Local
Settings
Factory Default
Click Check for Update to check if a remote update image is available.
Check for Update

Simply click **Check for Update** to get the information on if a new update is available on the update server.

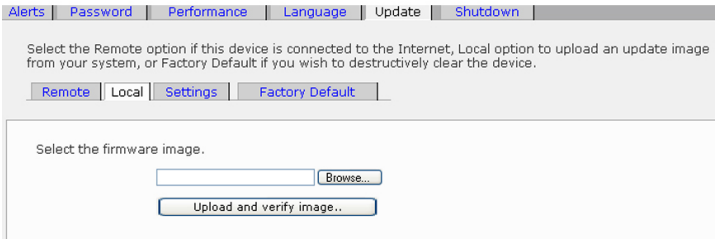


If you wish to continue, click **Perform System Update**. After the update image has been downloaded, you will be asked to reboot the system. The update process only updates the firmware image and does not modify your data volume. However, it is always a good idea to backup your important data whenever you perform an update.

LOCAL UPDATE

In situations where the TeraNAS device is not connected to the Internet, or Internet access is blocked, you can download an update file from the Support site and upload that file to the TeraNAS in the **Local** update tab.

System

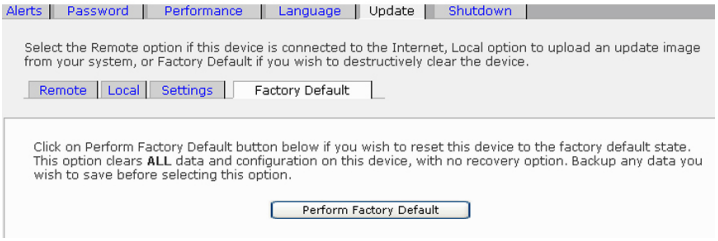


Click on the Browse button to select the update file and click the **Upload and verify image** button. The process will take several minutes at which time you will be requested to reboot the system to proceed with the upgrade. Do not click on the browser Refresh button during the update.

FACTORY DEFAULT

The **Factory Default** tab allows you to set the TeraNAS device back to factory default. Choose this option carefully, and remember to back up any data that you wish to keep.

System


Alerts
Password
Performance
Language
Update
Shutdown
Select the Remote option if this device is connected to the Internet, Local option to upload an update image from your system, or Factory Default if you wish to destructively clear the device.
Remote
Local
Settings
Factory Default
Click on Perform Factory Default button below if you wish to reset this device to the factory default state. This option clears ALL data and configuration on this device, with no recovery option. Backup any data you wish to save before selecting this option.
Perform Factory Default

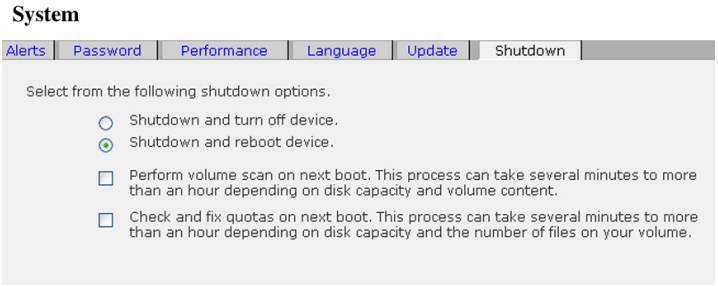
You will be asked to confirm your intention by typing: **FACTORY**

Warning

Performing Factory Default will wipe out everything, including data shares, volume, user and group accounts, and configuration information. There is no way to recover after you confirm this option.

Shutdown

The Shutdown tab offers the option to power-off or reboot the TeraNAS device.


System
Alerts
Password
Performance
Language
Update
Shutdown
Select from the following shutdown options.
Shutdown and turn off device.
Shutdown and reboot device.
Perform volume scan on next boot. This process can take several minutes to more than an hour depending on disk capacity and volume content.
Check and fix quotas on next boot. This process can take several minutes to more than an hour depending on disk capacity and the number of files on your volume.

You have the option of performing a full file system check or check quotas on the next boot. Both these options can take several minutes to several hours depending on the size of your volume and the number

of files in the volume. You do not need to select these options unless you suspect there might be data or quota integrity problems.

When you reboot or shutdown TeraNAS, you will need to close the browser window and use RAIDar to re-connect to FrontView.

Status

The Status page consists of the **Logs** and **Health** tabs providing system status information.

Logs

The Logs tab provides status information of management tasks along with timestamp.

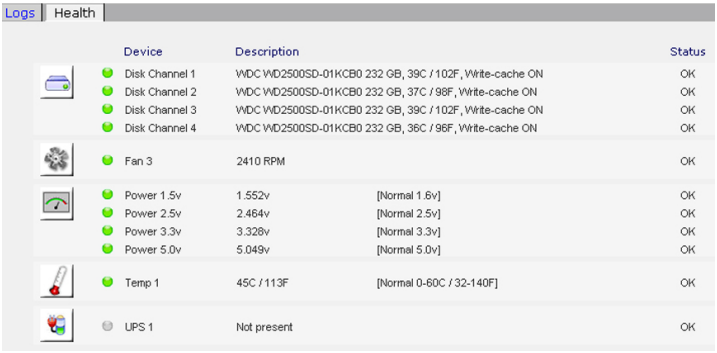
Status
Logs | Health |
Mon Jul 18 07:24:52 PDT 2005 The volume will not be added until you restart this device. This process can take 30 minutes or more depending on your volume size, during which you will not be able to access this device. You will be notified by email when the volume add process is complete.
Mon Jul 18 07:23:01 PDT 2005 The volume will not be added until you restart this device. This process can take 30 minutes or more depending on your volume size, during which you will not be able to access this device. You will be notified by email when the volume add process is complete.
Mon Jul 18 07:22:09 PDT 2005 Blinking disk 1
Mon Jul 18 07:15:08 PDT 2005 Snapshot successfully deleted.
Mon Jul 18 07:14:22 PDT 2005 Snapshot successfully taken.
Mon Jul 18 07:10:04 PDT 2005 Successfully applied security setting.
Mon Jul 18 07:04:43 PDT 2005 Successfully applied security setting.
Mon Jul 18 07:01:16 PDT 2005 Successfully started FTP service.
Mon Jul 18 07:01:14 PDT 2005 Successfully stopped Rsync service.
Mon Jul 18 07:01:13 PDT 2005 Successfully started FTP service.
Mon Jul 18 06:53:10 PDT 2005 Successfully applied security setting.
Mon Jul 18 06:44:56 PDT 2005 Successfully applied security setting.
Mon Jul 18 06:44:05 PDT 2005 Successfully applied security setting.
Mon Jul 18 06:37:46 PDT 2005 System is up.
Mon Jul 18 06:31:02 PDT 2005 Successfully changed admin password.
Mon Jul 18 06:21:38 PDT 2005 System is up.
Mon Jul 18 06:21:14 PDT 2005 Your NAS device has been updated with a new update image.
Mon Jul 18 06:17:12 PDT 2005 Please close this browser session and use RAIDar to reconnect to the device. System rebooting...
Mon Jul 18 06:16:01 PDT 2005 Please reboot your NAS device to continue with the update process.
Mon Jul 18 06:13:09 PDT 2005 Successfully applied security setting.
Mon Jul 18 05:25:49 PDT 2005 Alert contact(s) saved.
Mon Jul 18 05:25:36 PDT 2005 Alert contact(s) saved.

The **Send All Logs** button is available in case of problems where technical support personnel may be of assistance in analyzing low-level log information.

Health

The **Health** page displays the disk, fan, power, temperature, and UPS status in more detailed form than what is available in the Status bar. Where available, normal expected value range is provided.

Status

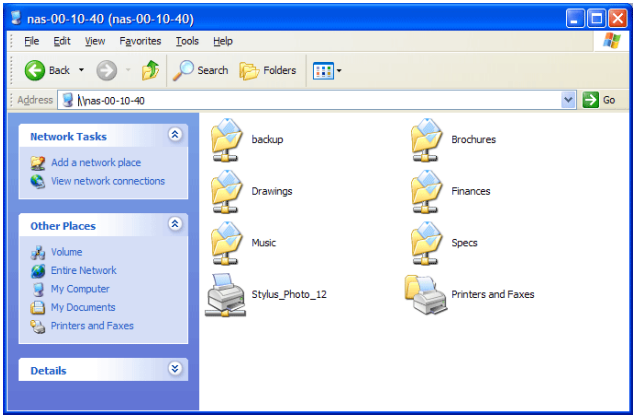

Logs
Health
Device
Description
Status
Disk Channel 1
WDC WD2500SD-01KCB0 232 GB, 39C / 102F, Write-cache ON
OK
Disk Channel 2
WDC WD2500SD-01KCB0 232 GB, 37C / 98F, Write-cache ON
OK
Disk Channel 3
WDC WD2500SD-01KCB0 232 GB, 39C / 102F, Write-cache ON
OK
Disk Channel 4
WDC WD2500SD-01KCB0 232 GB, 36C / 96F, Write-cache ON
OK
Fan 3
2410 RPM
OK
Power 1.5v
1.552v
[Normal 1.6v]
OK
Power 2.5v
2.464v
[Normal 2.5v]
OK
Power 3.3v
3.328v
[Normal 3.3v]
OK
Power 5.0v
5.049v
[Normal 5.0v]
OK
Temp 1
45C / 113F
[Normal 0-60C / 32-140F]
OK
UPS 1
Not present
OK

Chapter 2 Accessing Shares

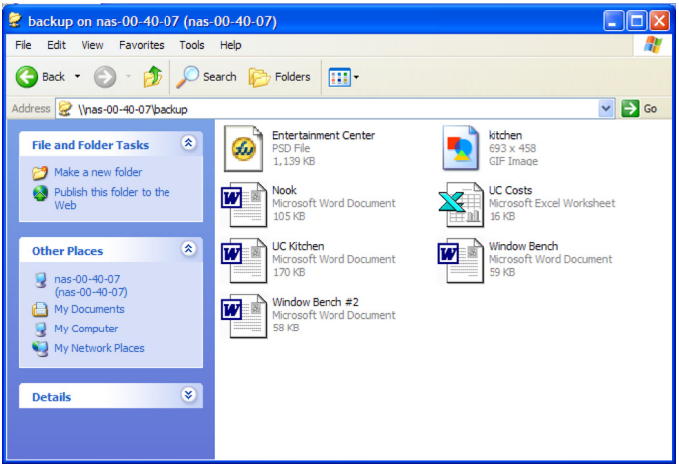
This chapter presents examples of how shares on this TeraNAS device can be accessed by the various operating systems. If you have problems accessing your shares, make sure to enable the corresponding service in the Shares Services tab. Also make sure to set the default access of the share to **Read-only** or **Read/write**.

Windows

To see a share listing under Windows, either click **Browse** in **RAIDar** or enter *hostname* or *ip_address* in the Explorer address bar. *Hostname* is the NAS hostname assigned in the Network tab. The default hostname is set to *nas-* followed by the last three hex bytes of the device MAC address.

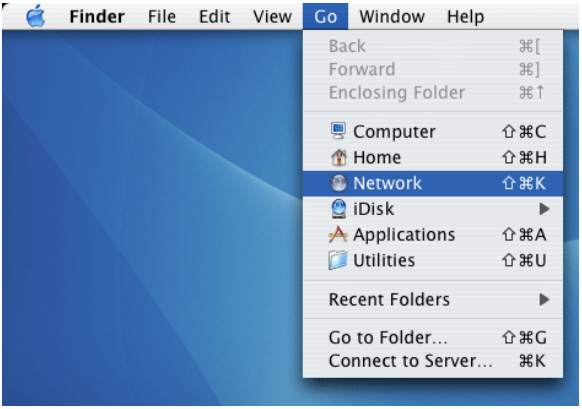


To access the share under Windows, specify the hostname followed by the share name in the Explorer address bar, i.e. *hostname*\backup, as follows:

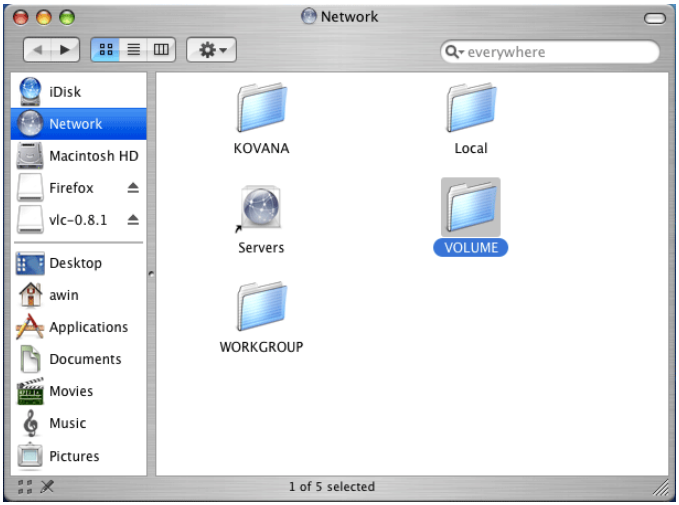


MAC OS X

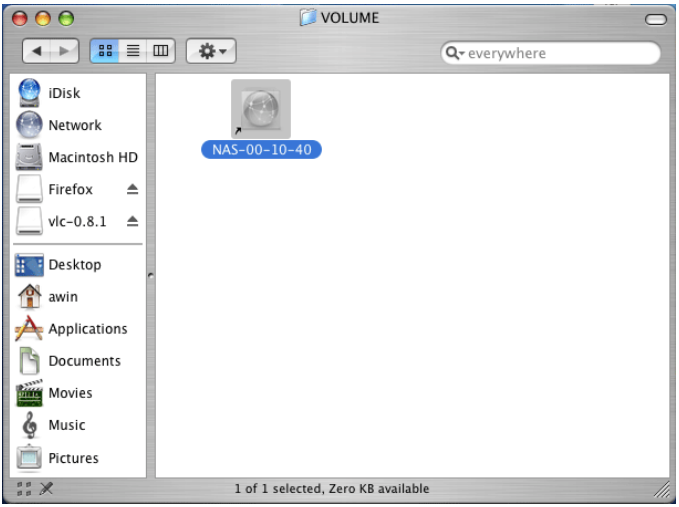
To access the same share under Mac OS X, select **Network** from the Finder **Go** menu.



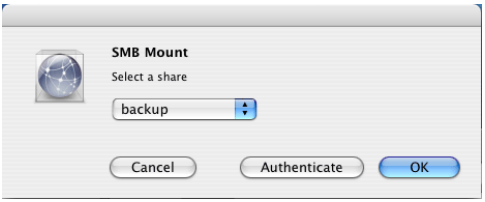
You will see a listing of available networks. The workgroup or domain name of the TeraNAS system will appear in the listing. If you left the name unchanged, you should see **Volume**.



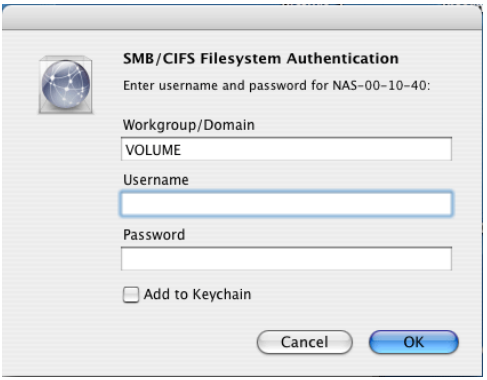
Double-click the workgroup or domain name icon to display the TeraNAS host name.



Double-click on the host name icon to display the share listing.

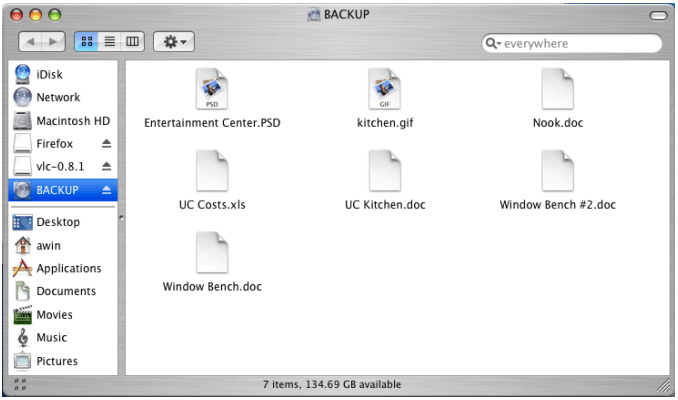


Select the share you wish to connect to and click **OK** to get the login prompt.



In **Share** security mode, you will need to only specify user name and password if you have set up a password for your share. Enter the share name in place of the user name. In **User** or **Domain** security mode, enter the user name and password you wish to connect to the TeraNAS as.

You should see the same file listing as you would in the Windows Explorer.



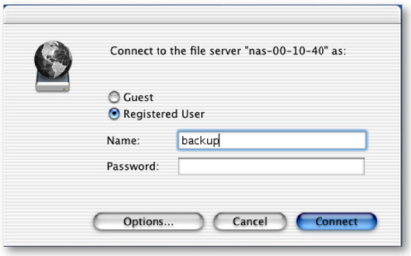
MAC OS 9

To access the same share under Mac OS 9, select Connect to Server from the Finder menu, choose the NAS device entry from the AppleTalk selection, and click **Connect**.

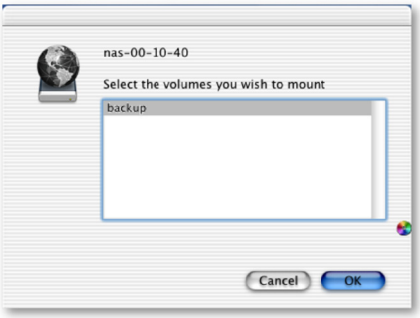
When you are prompted to login, enter the **share name** and **password** if the NAS is configured for **Share** security mode, or enter a valid user account and password otherwise.

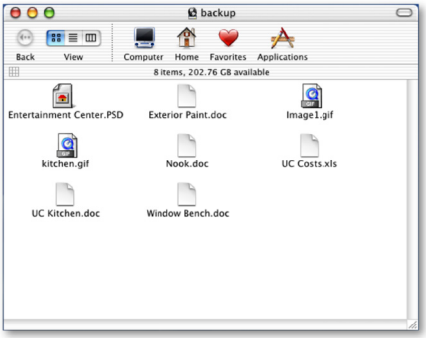
If no share password is set in **Share** mode, you can select **Guest** user and leave the password field blank.

If your login is successful, you will be given a listing of one or more shares. Select the share you wish to connect to.



You should see the same files in the share that you do under Windows.



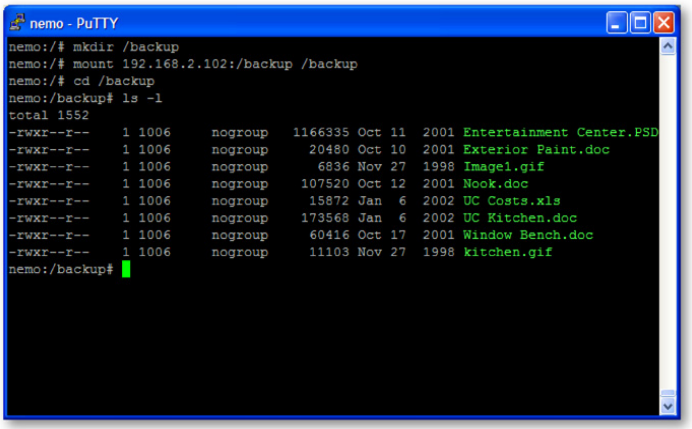


Linux / UNIX

To access this share from a Linux or Unix client, you will need to mount the share over NFS, i.e. type:

mount *ipaddr*:**/backup /backup**

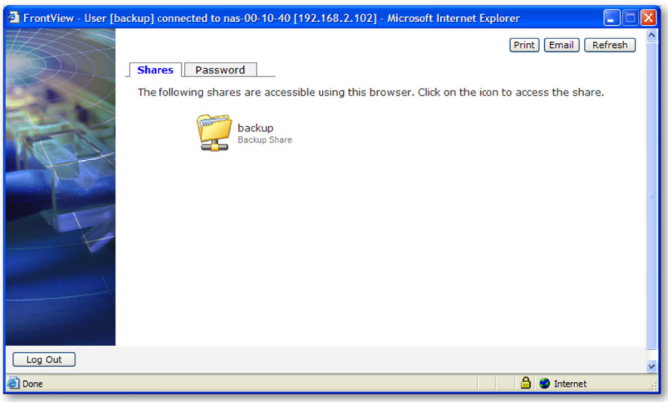
where **backup** is the share name. Running the **ls** command in the mounted path displays the share content.


nemo - PuTTY
nemo:/# mkdir /backup
nemo:/# mount 192.168.2.102:/backup /backup
nemo:/# cd /backup
nemo:/backup# ls -l
total 1552
-rwxr--r-- 1 1006 nogroup 1166335 Oct 11 2001 Entertainment Center.PSD
-rwxr--r-- 1 1006 nogroup 20480 Oct 10 2001 Exterior Paint.doc
-rwxr--r-- 1 1006 nogroup 6836 Nov 27 1998 Image1.gif
-rwxr--r-- 1 1006 nogroup 107520 Oct 12 2001 Nook.doc
-rwxr--r-- 1 1006 nogroup 15872 Jan 6 2002 UC Costs.xls
-rwxr--r-- 1 1006 nogroup 173568 Jan 6 2002 UC Kitchen.doc
-rwxr--r-- 1 1006 nogroup 60416 Oct 17 2001 Window Bench.doc
-rwxr--r-- 1 1006 nogroup 11103 Nov 27 1998 kitchen.gif
nemo:/backup#

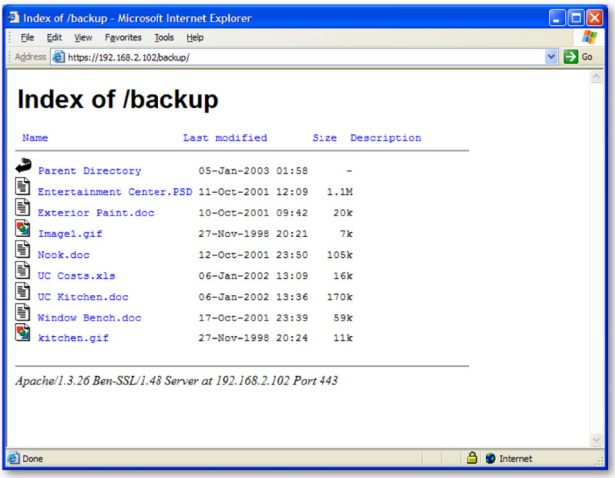
Web Browsing

To access the same share using a web browser, enter http://*ipaddr* in the browser address bar. You can use **https** if you want a secure encrypted connection. You will be prompted to login.

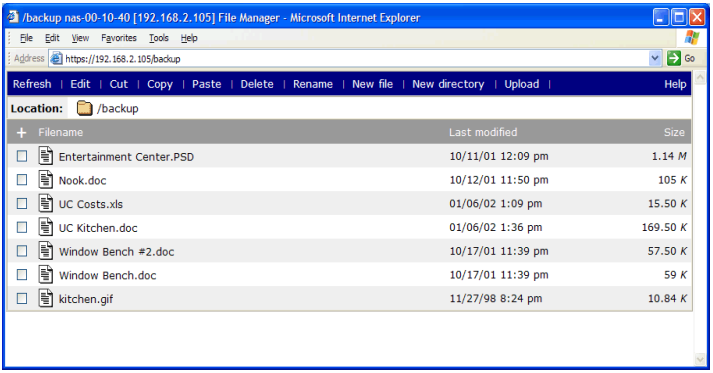
Enter the share name and share password if the TeraNAS is in **Share** security mode. Otherwise, login as a valid user and password if in **User** or **Domain** mode.



If the share access is read-only, the file manager will display:


Index of /backup - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://192.168.2.102/backup/
Go
Index of /backup
Name Last modified Size Description
Parent Directory 05-Jan-2003 01:58 -
Entertainment Center.PSD 11-Oct-2001 12:09 1.1M
Exterior Paint.doc 10-Oct-2001 09:42 20k
Image1.gif 27-Nov-1998 20:21 7k
Nook.doc 12-Oct-2001 23:50 105k
UC Costs.xls 06-Jan-2002 13:09 16k
UC Kitchen.doc 06-Jan-2002 13:36 170k
Window Bench.doc 17-Oct-2001 23:39 59k
kitchen.gif 27-Nov-1998 20:24 11k
Apache/1.3.26 Ben-SSL/1.48 Server at 192.168.2.102 Port 443
Done
Internet

If the share is writable, the file manager will have options for creating, modifying, and deleting files, as follows:


/backup nas-00-10-40 [192.168.2.105] File Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://192.168.2.105/backup
Go
Refresh | Edit | Cut | Copy | Paste | Delete | Rename | New file | New directory | Upload | Help
Location: /backup
Filename Last modified Size
Entertainment Center.PSD 10/11/01 12:09 pm 1.14 M
Nook.doc 10/12/01 11:50 pm 105 K
UC Costs.xls 01/06/02 1:09 pm 15.50 K
UC Kitchen.doc 01/06/02 1:36 pm 169.50 K
Window Bench #2.doc 10/17/01 11:39 pm 57.50 K
Window Bench.doc 10/17/01 11:39 pm 59 K
kitchen.gif 11/27/98 8:24 pm 10.84 K

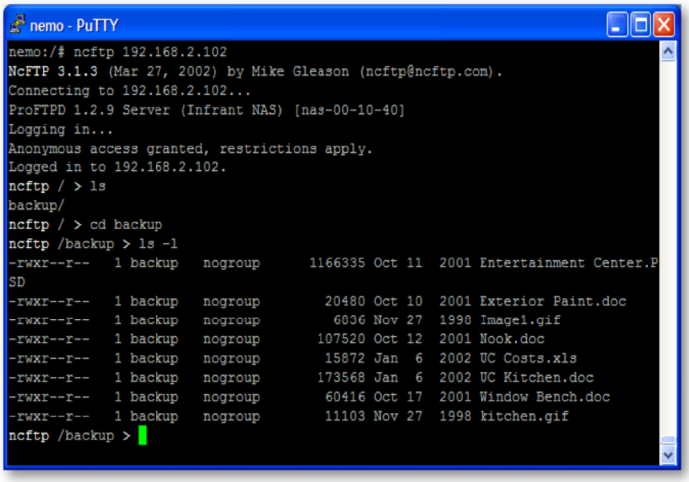
One useful application for a web share is for setting up a company intranet. You can copy HTML files to the web share using Windows, Mac, NFS, or HTTP. When you set HTTP access to read-only, html files, including index.htm and index.html, can be viewed using any web browser.

Note

Files created under the Web file manager can only be deleted under this file manager. Files not created from this file manager can be modified but cannot be deleted here.

FTP

To access this same share with FTP, you can use anonymous login and access the share.


nemo - PuTTY
nemo:/# ncftp 192.168.2.102
NcFTP 3.1.3 (Mar 27, 2002) by Mike Gleason (ncftp@ncftp.com).
Connecting to 192.168.2.102...
ProFTPD 1.2.9 Server (Infrant NAS) [nas-00-10-40]
Logging in...
Anonymous access granted, restrictions apply.
Logged in to 192.168.2.102.
ncftp / > ls
backup/
ncftp / > cd backup
ncftp /backup > ls -l
-rwxr--r-- 1 backup nogroup 1166335 Oct 11 2001 Entertainment Center.P
SD
-rwxr--r-- 1 backup nogroup 20480 Oct 10 2001 Exterior Paint.doc
-rwxr--r-- 1 backup nogroup 6036 Nov 27 1990 Image1.gif
-rwxr--r-- 1 backup nogroup 107520 Oct 12 2001 Nook.doc
-rwxr--r-- 1 backup nogroup 15872 Jan 6 2002 UC Costs.xls
-rwxr--r-- 1 backup nogroup 173568 Jan 6 2002 UC Kitchen.doc
-rwxr--r-- 1 backup nogroup 60416 Oct 17 2001 Window Bench.doc
-rwxr--r-- 1 backup nogroup 11103 Nov 27 1998 kitchen.gif
ncftp /backup >

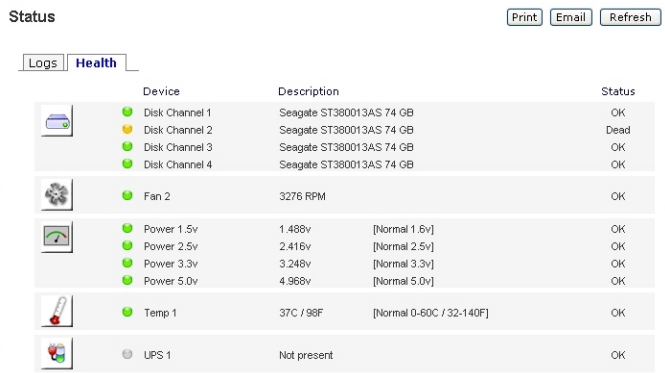
Note that enabling FTP access to the share opens up access to your data to anyone who has a FTP client on your network. It is best to enable FTP access only to shares you are comfortable making public on your network.

Also note that disk usage using FTP will not count towards the share disk quota, so again, choose how you advertise a share over FTP carefully.

Chapter 3 Replacing a Failed Disk

Locate the Failed Disk

When a disk fails in your TeraNAS device, you will be notified of the failure by email. The failed disk location can be seen in the FrontView status bar at the bottom.



If you look at the front of the TeraNAS device, you can also determine the failed disk location by the amber LED that is lit. The left-most LED is disk channel 1, the next one is disk channel 2, and so on. Take note of the failed channel.

Order Replacement Disk

Go to the TeraNAS system. It is best to replace a failed disk with the same disk model. Contact the disk vendor and arrange to have the disk replaced if the disk is still under warranty. Disk RMA from the vendor will require that you provide the serial number of the disk, so you will need to open the case and take out the failed disk to get this info. See the next section on how to do this.

If the disk is no longer under warranty, you can obtain a disk of the same capacity or larger from your TeraNAS retailer.

Replace the Failed Disk

Shutdown the TeraNAS and open up the enclosure as instructed in the **Getting Started** guide. If you view the disks from the front of the enclosure, the left-most disk is channel 1, the next disk is channel 2, and so on.

You will need to remove the drive cage and disconnect the power and SATA cable from the failed disk. Insert the new replacement disk, reconnect the cables, insert the drive cage, and secure the enclosure.

Warning

When replacing the cables, make sure the connectors fit **squared-on** and **securely**. After the drive cage is re-inserted, double-check the connectors to make sure they have not come loose. Loose connection may cause spurious drive failure events that may render the data volume dead.

Resynchronize the Volume

Power on the TeraNAS. The RAID volume will automatically resync data onto the new disk in the background. The process will take several hours depending on disk size. During the resync process, the TeraNAS can be used as normal, although access will slow down from normal speed.

You will be notified by email when the resync process is complete.

Chapter 4 System Reset Switch

Refer to the Getting Started guide included in the shipping box for the location of the **System Reset** switch on the back of the TeraNAS.

The System Reset switch allows you to perform two tasks: (1) re-install the TeraNAS firmware and (2) set TeraNAS back to factory default mode. Typically, you should not need to resort to either option unless you have exhausted all means to recover your system. You may want to re-install the TeraNAS firmware as a first step if the TeraNAS had been working normally and you have some configuration change which made it no longer respond. If this does not work and/or you wish to set the TeraNAS back to a factory default state, you can do so following the Factory Default instruction below.

- **To re-install the TeraNAS firmware**, use a paper clip to depress the switch while Power Switch is off, and maintain for 5 secs after the Power Switch is turned on. The disk LEDs will turn on once to signify that the command has been accepted. The firmware installation will take several minutes to complete. The Status LED in the front will be on solid when the process is complete. The installation will not affect the data on the TeraNAS, **but make sure not to press the switch for too long, otherwise a destructive Factory Default process will be done instead** (see below).
- **To set the TeraNAS device to Factory Default**, use the same process, except depress the System Reset Switch for 30 secs. You should see the disk LEDs blink a second time to signify that the command has been accepted. Note that this process re-installs the firmware and resets all disk configuration, wiping out any data you may have on the NAS.

For both activities, make sure to back up important data before starting.

Appendix A Streaming Videos Using SnaZio* Tera NAS HD Pro

Introduction

Having a complete Network Attached Storage with streaming capabilities is an ideal solution for those people who have been looking to archive and stream their huge collections of videos to their network media players. SnaZio* Tera NAS HD provides them a way to manage and stream their vast amounts of digital media contents. It's designed to manage multiple connected embedded devices securely across the network.

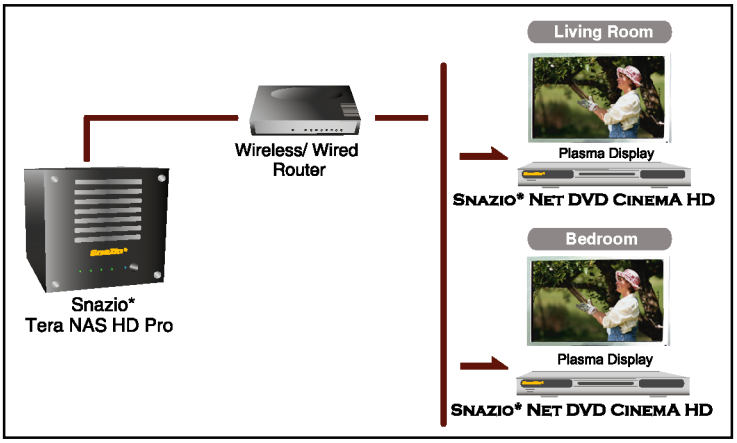
SnaZio* Tera NAS comes together with Snazzi Net Cinema software which helps it to be a complete media management and streaming device to watch your media contents on SnaZio* NetDVD Cinema HD. In this appendix we will discuss how to setup a Tera NAS as a Media Streaming Server.

Network Connections

SnaZio* Tera NAS can be either used via wired or wireless network. For wired networking, there are two possibilities. Either you connect Tera NAS directly with your Network media player or you first connect it with a Hub in between.

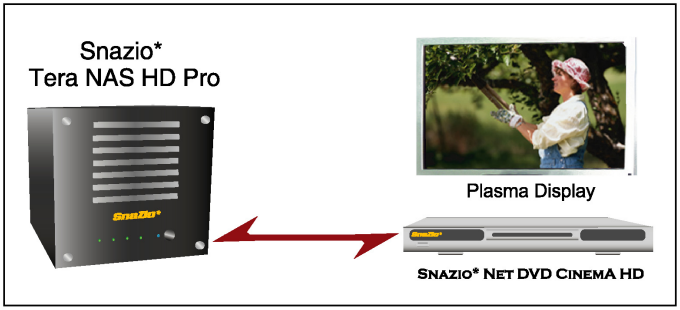
Connecting Via HUB: Use a supplied LAN cable that comes with the package to connect your SnaZio* Tera NAS with hub. The same hub is

also connected with the different network media players who can access the Tera NAS simultaneously.



Connecting Directly To a SnaZio* Player: Use a Cross-over cable to directly connect SnaZio* Tera NAS with your SnaZio* NetDVD Cinema HD player. Your IP address class must be the same. Cross-over cable is not included in the package.

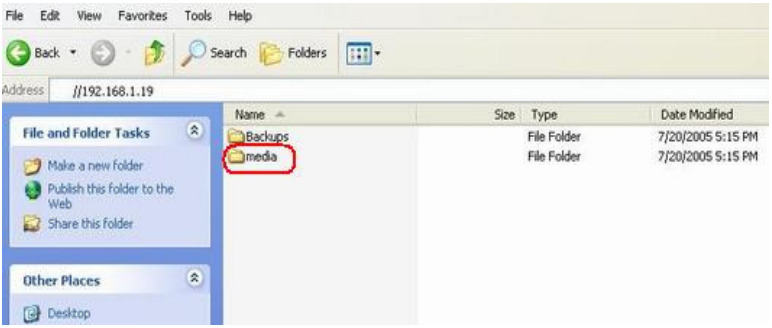
Either provide a Static IP address to the Tera NAS so that later you can access it from the player side or set the Tera NAS to work as a DHCP server and the player will automatically take the IP from the Tera NAS.



For wireless you have to connect the Tera NAS to your wireless access point with Ethernet cable or you can connect a USB wireless adaptor. For more information on setting up networking options for Tera NAS firmware, refer to Page 13-15 of the Tera NAS User's Manual.

Managing Media Contents

As mentioned earlier there is no need to install any kind of software. After RAID synching, SnaZio* Tera NAS will automatically create default shares. These default shares are named as "Backup" and "media" and can be used for media management. You can check the shares by accessing NAS.



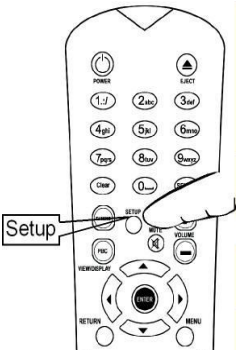
Access the Tera NAS and make sure that "media" folder is available. Create three sub-folders manually inside "media" and name them as "Music", "Pictures" and "Videos"

NOTE: If there is no share upon accessing Tera NAS, Add a share named "media" manually as explained on Page-20 of the Quick Installation section of the User Guide. Please make sure to follow the same naming convention for folders.

Copy all your media files you want to archive in the relevant folders. At any time, you may increase the quota for the **"media"** share by easy to use web-management panel. Just go to the Share Tab and increase the quota specified on the right side, click apply for the changes to take effect.

Playing Media Files

SnaZio* Tera NAS will be automatically detected by SnaZio* NetDVD Cinema HD and will appear in the login page. Select the Tera NAS and press **"Enter"** button on the NetDVD remote control to browse for the Videos, Music and Photos menu.



Select the type of the media content you want to play from the Welcome Page and click **"Enter"** to proceed.

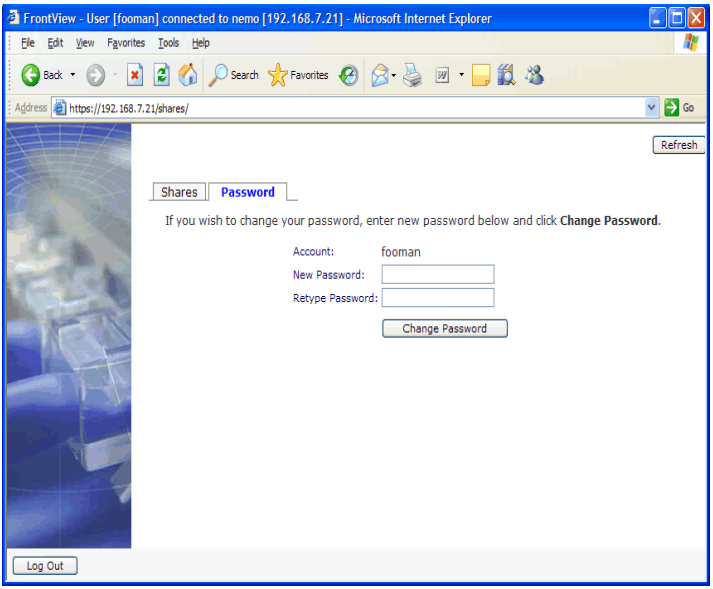
A list of all the media files in selected category will be displayed on your remote player. For example if you browse Video category, all the files you have copied in the **"media-Videos"** folder on your Tera NAS will be displayed. Choose a file and click **"Enter"** on your Remote Control or Click **"Play All"** to start playing all the video files in a folder.

Use the standard playback controls on the SnaZio* Net DVD Cinema's Remote Control. The same way is also applicable to play audios and Music files.

Appendix B Changing User Password

There are two ways in which user passwords can be changed in **User security mode**. The first way is for the admin user to change the passwords in the **Accounts** tab in the **Security** menu. The preferable way is to allow users to change their passwords on their own. This alleviates the admin of a common occurrence and encourages the users to change their passwords on a regular basis for better security.

Users can use the web browser and log in to *https://ip_addr/* to access the web share listing page and select the **Password** tab. There, a new password can be set.



In **Share** and **Domain** security mode, the **Password** tab will not appear. User passwords in **Domain** mode must be set on the domain or ADS server.

Appendix C RAID Levels Simplified

RAID can be somewhat daunting, so without going into too much details, this chapter will help simplify RAID for you.

RAID is an acronym for **R**edundant **A**rray of **I**ndependent **D**isks. Basically it is a method of storing data on multiple disks in a way that if

one disk fails, data can still be accessed from the surviving disk(s). A RAID level selects how data will be kept redundant, the most popular ones being levels 0, 1, and 5. Contrary to the RAID acronym, RAID level 0 does not provide any redundancy.

RAID Level 0

RAID level 0 provides the best write performance of all the RAID levels as it stripes data across all disks so that data can be written to all disks in parallel. Unfortunately, it is not redundant, so if one disk fails the entire volume will be dead. RAID level 0 can be configured with one or more disks, and its capacity is the size of the smallest disk in the RAID set multiplied by the number of disks in the set. For example, a four disk RAID 0 will yield the capacity of all four disks, assuming they are identical in size.

RAID Level 1

RAID level 1 consists of 2 or more disks, all disk(s) other than the first being an exact mirror of the first. RAID level 1 can sustain disk failure up to the total number of disks in the RAID set minus one. For example, a two-disk RAID 1 volume can sustain a one-disk failure and continue running. A three-disk RAID 1 volume can sustain up to two disk failures. If a disk fails, the data is retrieved from the surviving disk. Unfortunately, RAID 1 capacity utilization is not optimal in a three or more disk configuration. The capacity is limited to the size of the smallest disk in the RAID set.

RAID Level 5

RAID level 5 provides the best balance of capacity and performance while providing data redundancy. RAID 5 provides redundancy by striping data across three or more disks and keeping the parity information on one of the disks in each stripe. In case of disk failure, the surviving disks and the parity disk are used to reconstruct the lost data, providing that data transparently to the user application. Upon replacing the failed disk with a good disk, the reconstructed data is written out to the new disk, and when the reconstruction (or sometimes referred as resync) process is complete, the volume returns to a redundant state. The capacity of a RAID 5 volume is the smallest disk in the RAID set multiplied by one less than the number of disks in the RAID set. For example, a four-disk RAID 5 set will provide the capacity of three disks, assuming all four disks are identical in size.

Appendix D Input Field Format

Domain/Workgroup Name

A valid domain or workgroup name must conform to the following restrictions:

- Name must only consist of characters a-z, A-Z, 0-9, and the symbols _ (underscore), – (dash), and . (period).
- Name must start with a letter.
- Name length must be 15 characters or less.

Host

A valid IP address or a host name.

Host Name

A valid host name must conform to the following restrictions:

- Name must only consist of characters a-z, A-Z, 0-9, and the symbols – (dash) and . (period).
- Name must start with a letter.
- A short host name length must be 24 characters or less.
- A fully-qualified domain name (FQDN) must have no more than 24 characters in each section separated by . (period), and cannot end with a – (dash). Example of a valid FQDN: firstpart.secondpart.thirdpart.com.

TeraNAS Host Name

A valid host name except the first part or short host name must be 15 characters or less due to NetBIOS name length restriction.

Host Expression

A valid host expression is either a valid host or the common IP expression form specifying a range of addresses in a network; for example:

- 192.168.2.
- 192.168.2.0/255.255.255.0

- 192.168.2.0/8

Share Name

- Name must only consist of characters a-z, A-Z, 0-9, and the symbols – (dash) and . (period).
- Name cannot be an existing user name.
- Name cannot end in *–snap*.
- Name cannot be any one of the following reserved names:

```
bin boot cdrom dev etc floppy frontview home
initrd lib lost+found mnt opt proc root sbin
tmp usr var admin administrator images
language quota.user quota.group shares global
homes printers c d e f g h i j
```

Share Password

- Any character except for ‘ (single quote).
- Share passwords are limited to 8 characters.

SNMP Community

- Name must only consist of characters a-z, A-Z, 0-9, and the symbols – (dash) and . (period).
- Name must start with a letter.
- Name length must be 32 characters or less.

User/Group Name

- Name must only consist of characters a-z, A-Z, 0-9, and the symbols _ (underscore), – (dash), @, and . (period).
- Name cannot be an existing share name.

User Password

- Any character except for ‘ (single quote).

Appendix E Glossary

AFP: AppleTalk Filing Protocol, is the standard way Mac OS 9 and earlier share files across the network.

CIFS: Common Internet File System, a standard protocol that Windows users use to share files across the network. Mac OS X also has the capability to share files using CIFS.

FTP: File Transfer Protocol, a common protocol adopted by many OS to enable remote file download and upload for public sharing.

HTTP: Hypertext Transfer Protocol, the protocol web browsers use to connect to web servers for file access, typically web pages.

HTTPS: HTTP with SSL encryption, is used where secure web access is desired.

NFS: Network File System, a common way Unix and Linux systems share files by making remote file systems appear to reside locally.

Quota: Amount of volume space allocated to a particular user or group account, or to a particular share. The user, group, or share with a set quota cannot exceed disk usage beyond this limit. Quota is typically specified to ensure no one user, group, or share will abuse the available storage space.

RAID: Acronym for **R**edundant **A**rray of **I**ndependent **D**isks. Basically it is a method of storing data on multiple disks in a way that if one disk fails, data can still be accessed from

the other disk(s). A RAID level selects how data will be kept redundant, the most popular of which are levels 0, 1, and 5. Contrary to the RAID acronym, RAID level 0 does not provide any redundancy. For more info, see **RAID Levels Simplified** in **Appendix A**.

Share: A folder on a NAS volume that can be shared amongst different network file services such as CIFS for Windows, AFP (AppleTalk File Protocol) for Macs, NFS for Unix/Linux, FTP, and HTTP. Access to the share can be customized on a user/group/host-level basis.

Snapshot: An instantaneous, non-changing, read-only image of a volume. Snapshots are useful for backups during which time the original volume can continue to operate normally. Snapshots can also be utilized as a temporary backup against viruses. Files can be restored from the snapshot volume if current files are corrupted.

Volume: A filesystem built on top of a RAID set. This filesystem consists of shares that are made available through various network file services.

Appendix F If You Need Help...

If you have questions or you encounter problems with the setup, you can visit our support site at http://www.Snazio.com There, you'll find links to FAQs, message board, and live online support. During off-hours, you can post questions on the message board which is frequented by advanced users and V One Multimedia engineering support and design staff.